Universidad Carlos III de Madrid

Escuela Politécnica Superior

Grado en Ingeniería Telemática

DESPLIEGUE DE UNA INFRAESTRUCTURA PARA EL ANÁLISIS DEL TRÁFICO 802.11

Trabajo Fin de Grado

Autor: **José María Montes Yuste**
Tutor: **Pablo Serrano Yáñez-Mingot**
Director: **Andrés García Saavedra**

Julio 2013

Trabajo Fin de Grado

Despliegue de una infraestructura para el análisis del tráfico 802.11

Autor:

José María Montes Yuste

Tutor:

Pablo Serrano Yáñez-Mingot

Director:

Andrés García Saavedra

Realizado el acto de defensa y lectura del Trabajo Fin de Grado el día 10 de julio de 2013 en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, el tribunal:

Presidente:

Secretario:

Vocal:

acuerdan otorgarle la calificación de:

Calificación:

Leganés, a 10 de julio de 2013

A mis padres, a mi hermana y a Cristina.

Agradecimientos

En primer lugar agradecerles a mis padres y a mi hermana el apoyo y cariño que me han dado siempre, y que ha conseguido convertirme en la persona que soy hoy. También dar las gracias a Cristina que sin ella nada de esto sería posible.

Agradecer a mis tutores Andrés, Pablo y Carlos todo vuestro apoyo y tiempo dedicado. Por mostrarme el camino de la investigación.

Dar las gracias a todos los compañeros que he tenido a lo largo de estos años en la universidad, sin los cuales el camino hasta aquí hubiera sido mucho más duro. En especial a Daniel, por ser un extraordinario compañero. Hemos pasado muchos momentos juntos, unos mejores que otros, pero siempre hemos logrado encontrar el camino. Una parte se la debo a mis compañeros becarios en France Telecom, que me han hecho pasar un curso mucho más entretenido y ameno.

"El progreso y el desarrollo son

imposibles si uno sigue haciendo las cosas

tal y como siempre las ha hecho"

Wayne W. Dyer (1940)

Resumen

Durante los últimos años nos hemos convertido en una sociedad cada vez más móvil. Debido a esto, las formas tradicionales de comunicación se están quedando obsoletas. Los usuarios demandan una comunicación y conexión a la red libre, sin necesidad de estar conectados físicamente con un cable a la red. Estas necesidades son cubiertas por las redes inalámbricas, y en particular las redes WiFi. Existen estudios que demuestran un aumento de este tipo de redes en los últimos años, y uno aun mayor en años próximos. Algunas de las ventajas de estas redes, aparte de libre movilidad y circulación de usuarios mencionada ya anteriormente, son su bajo coste - en cuanto a la instalación de la infraestructura y su despliegue- , su versatilidad a la hora de dar servicio a múltiples dispositivos (smartphones, PDAs, ebooks, tablets, etc.), su presencia en muchos lugares públicos (como aeropuertos, centros comerciales, estaciones, oficinas, etc.), su fácil complementación con otro tipo de redes, etc. Pero si bien es necesario gestionar y administrar las redes cableadas, es todavía más importante hacerlo con las redes inalámbricas. El principal motivo es que la información, al carecer de cables que conectan los dispositivos entre sí, circula libremente por el medio aéreo, por lo que está al alcance de cualquier usuario con capacidades para capturar dicho tráfico. Gracias a la gestión y monitorización de la red se pueden detectar ataque de intrusos, identificar usuarios, detectar zonas de baja cobertura, mostrar información del uso de la red, prevenir posibles fallos por caída de equipos, etc. Por esto es necesario llevar una monitorización de la red, para hacer una gestión y administración lo más optima posible para el sistema.

Basándose en estas necesidades se ha realizado este Trabajo Fin de Grado, en el que se ha diseñado e implementado un sistema para el análisis del tráfico 802.11. El sistema consiste en el despliegue de una serie de nodos inalámbricos por el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid, que están encargados de monitorizar el tráfico que se produce en las zonas por las que están desplegados, para posteriormente poder analizar y gestionar de manera eficiente la red.

El proyecto de implementación de este sistema en el Departamento se puede dividir en las siguientes etapas. La primera de ellas consiste en, por un lado, configurar los nodos inalámbricos para automatizar las tareas de monitorización y, por otra parte, un servidor que los controle y en el que almacenar la información recogida. Este proceso se realiza mediante un registro de los nodos en el servidor, un envío de órdenes por parte del servidor especificas para cada nodo, y un almacenamiento de los datos recogidos por los nodos en el servidor. En la segunda etapa se despliegan los nodos por el Departamento, de manera que se intenta cubrir el mayor área posible para tener información representativa del tráfico de la red. Durante un mes y medio aproximadamente se va a monitorizar el trafico de la red y almacenar dicha información en el servidor. Finalmente con todos los datos recogidos, y con el fin de comprobar el correcto funcionamiento del sistema y mostrar alguna de las aplicaciones prácticas que se pueden llevar a cabo gracias a este sistema, se realiza un breve análisis de los datos para obtener cierta información relevante de la red. Estos datos se analizan de tres manera, una primera en la que se implementará una aplicación web para visualizar los datos en tiempo real; mediante mapas de gradientes que

muestren tráfico de la red; y con graficas que muestran la carga de las zonas controladas por los nodos.

Abstract

In recent years the world has evolved into an increasing mobile society. Because of this, traditional ways of communication are becoming obsolete. Users demand a certain freedom in their communication and in his communication networks, without the requirement of being physically connected with cable to the network. The wireless networks meet these needs, particularly WiFi networks. Some studies show an increase in this type of networks during last the years, and larger success in future years. Some of the advantage of these networks, besides free mobility and circulation of users already mentioned above, are the low cost in terms of infrastructure and deployment, its versatility to provide service to multiple devices (smartphones, PDAs, ebooks, tablets, etc..), its presence in many public places (airports, malls, stakes, offices, etc..), even as a complement to wired networks, etc.. Its really necessary to manage and administer wired networks but is even more important to do with wireless ones. The main reason for this need is that information, due to the lack of wires to provide connectivity, flows through the air, so it is available to any user with capabilities to capture that traffic. Thanks to the management and monitoring of these networks, we can detect attacks to the network, identify users, identify areas of low coverage, show information about network usage, prevent possible failures, etc. For all the stated above this thesis claims that network monitoring is necessary in order to provide the optimal management and administration possible of the network.

This thesis has been elaborated motivated by the above needs to designed and implemented a system to analysis traffic 802.11. The system consists of the deployment of a certain number of wireless nodes in the Department of Telematics of the University Carlos III of Madrid. These nodes have the responsibility of monitoring the traffic that flows in these areas where they are deployed, for a posteriori analysis and could manage the network efficiently.

The system can be divided into the following stages. The first is to configure the wireless nodes to automate the tasks of monitoring, and a server to store the information of the network. This process is executed by a register of the nodes in the server, then the server transfer specific orders to each of node, finally the nodes store that collected data on the server. In the second stage, the nodes are deployed by that Department, intended to cover all areas. The monitoring system has been active for a month and a half is going to monitoring the network capturing traffic and storing this information on the server. Finally, with all the data collected, and in order to check the correct operation of the system and show some of the applications that can be carried out thanks to him, an analysis is performed to get some information. These data are analyzed in three ways, the first with application web (is implemented to display the data in real time), using gradient maps of the network traffic, and with graphics that show the load of the network.

Índice general

Lista de figuras

Parte I

Introducción

I. Introducción

Este documento describe el proyecto realizado como Trabajo Fin de Grado, consistente en el diseño de una infraestructura para el análisis del tráfico 802.11 [1] y su correspondiente implementación y despliegue práctico.

1. Redes inalámbricas

En los últimos años el mundo se ha vuelto cada vez más móvil [2]. Por lo que las formas tradicionales de creación de redes están resultando insuficientes para afrontar los nuevos retos planteados por esta nueva forma de vida. Si lo usuarios tuvieran que estar conectados a la red por cables físicos su movilidad se vería muy reducida. Por ello la conectividad inalámbrica resulta crucial, permitiendo una gran libertad de circulación a los usuarios. Por esto, las tecnologías inalámbricas están invadiendo el ámbito de las redes actuales.

Masivo crecimiento de redes inalámbricas en los últimos tiempos.

Según el estudio realizado por Cisco [3], ha quedado demostrada la importancia en la sociedad actual – y futura – de las tecnologías inalámbricas. Este estudio refleja que el tráfico móvil a nivel mundial creció un 70 % en 2012, llegando a alcanzar los 885 petabytes el mes. En cuando a cantidad de tráfico, llegó casi a duplicar valores del año anterior. El consumo promedio de los smartphones creció un 81% en 2012. A nivel mundial, el 33% del tráfico total se descarga sobre redes Wi-Fi. Se estima que en los próximos cinco años el tráfico móvil alcance valores superiores a los 10 exabytes (un incremento de trece veces el actual). El número de dispositivos conectados superará a la población mundial, el 50% del tráfico generado será con smartphones. Se estima que 21 exabytes de tráfico de datos será descargado por redes Wi-Fi.

Una previsión de crecimiento aún mayor a medio plazo.

Como bien se observa en la Figura 1, se prevé una tendencia creciente del tráfico móvil durante los próximos cinco años [3]. Se estima que este crecimiento va a ser a nivel mundial, aunque bien es cierto que en las zonas más desarrolladas del planeta su crecimiento, y su uso, van a ser mucho más elevados, como muestra la Figura 2 . También cabe destacar que la utilización de esta tecnología, aunque se va a centrar en dispositivos tipo smartphones, no van a ser los únicos que sufran dicho crecimiento, sino que se va a producir un aumento similar en el resto de dispositivos capaces de soportar esta tecnología, como se muestra en la Figura 3. Todo esto nos lleva a estar en situación de afirmar que las redes inalámbricas, en los próximos años, van a sufrir un proceso de crecimiento bastante importante en todo el planeta, gracias en parte a que son soportadas por múltiples dispositivos móviles.

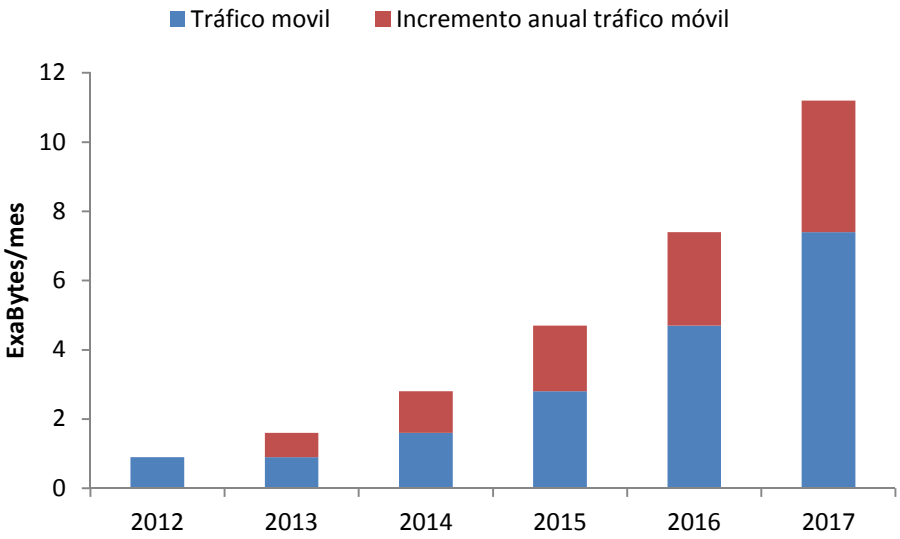


Figura 1 - Previsión de datos de tráfico móvil

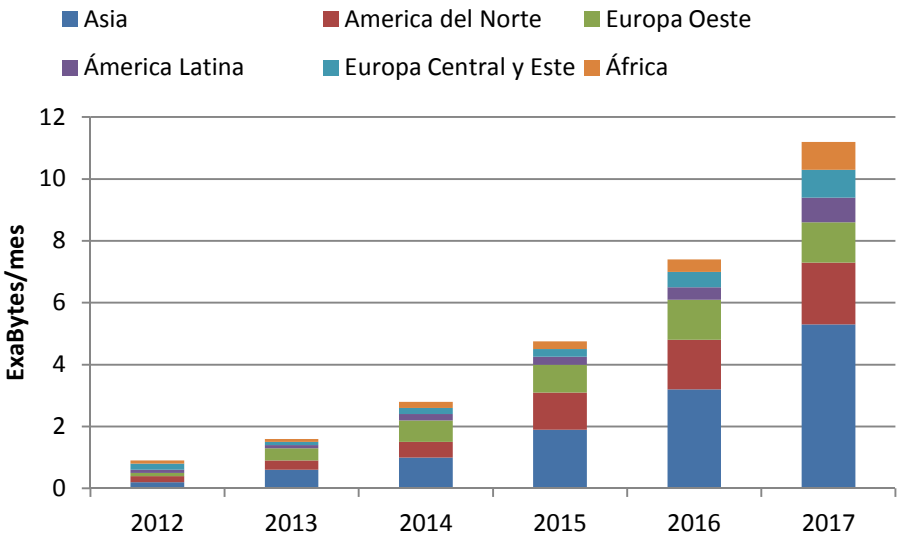


Figura 2 - Previsión de trafico móvil por zonas del planeta

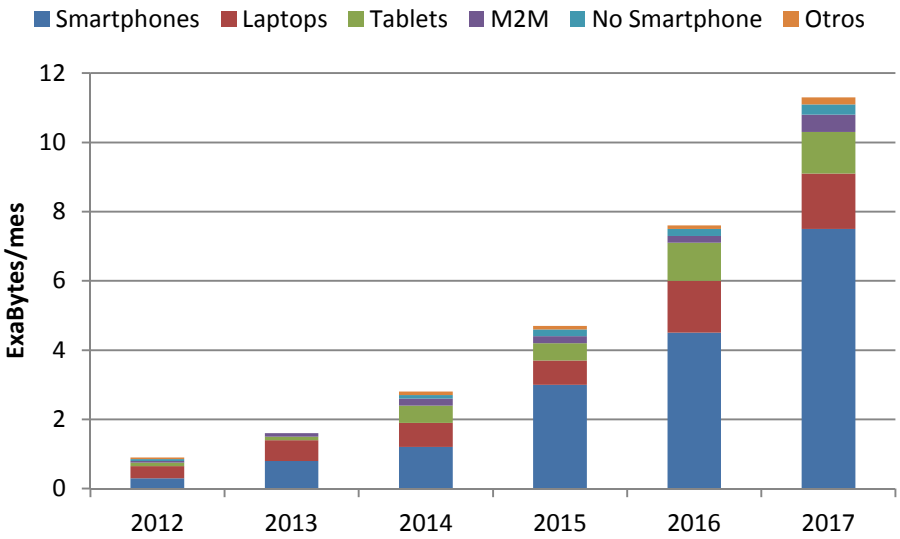


Figura 3 - Previsión tráfico móvil por tipo dispositivo

Diferentes tipos redes inalámbricas

Las redes inalámbricas, a diferencia de las cableadas, no necesitan una conexión fija a un punto terminal de la red, sino que, en este caso, la comunicación con la red se realiza mediante transmisiones radio [4]. El uso más frecuente que se da a las redes inalámbricas es para facilitar la movilidad de los usuarios, no para sustituir las redes cableadas. (En un futuro a corto-medio plazo se está pensando en la posibilidad de sí poder llegar a sustituirlas debido a sus múltiples ventajas, principalmente por su menor coste y su fácil despliegue en situaciones de emergencia. Incluso se plantea reemplazar parte del backbone de la red por infraestructuras inalámbricas [5]). Dependiendo de la aplicación que se le vaya a dar existen diferentes tipos de redes inalámbricas, en la Figura 4 se especifica su clasificación según el área de cobertura.

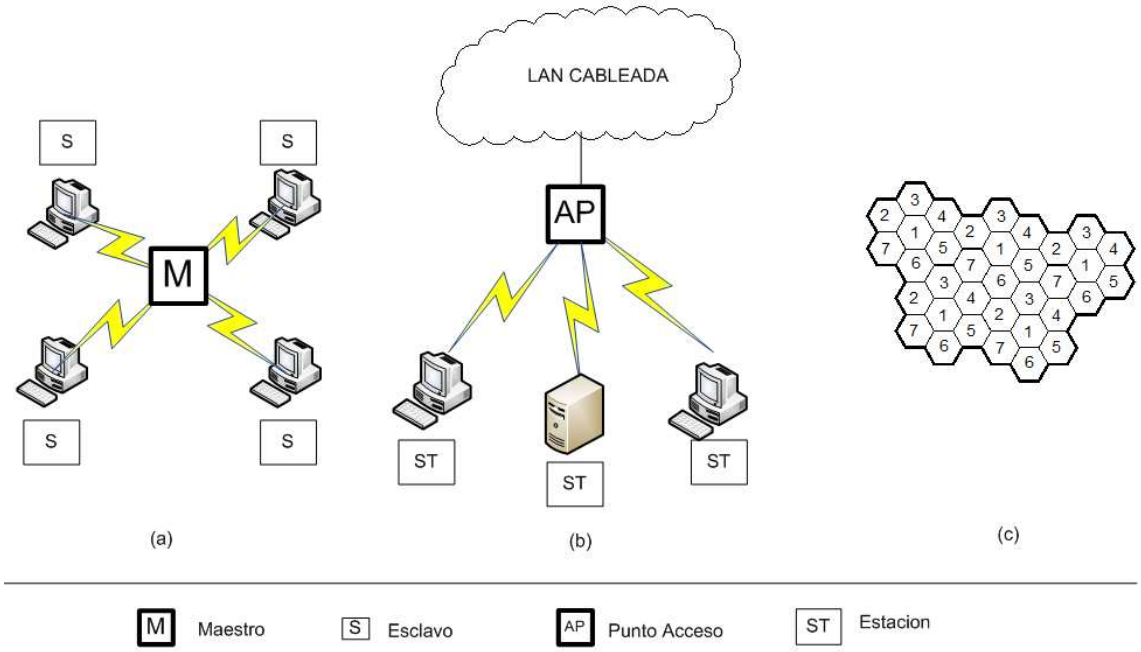


Figura 4 – Topologías redes inalámbricas por área de cobertura

La Figura 4.a corresponde a un modelo ad-hoc, en el que un dispositivo actúa como maestro, y el resto como esclavos [4]. Estos últimos deben estar conectados al maestro con una distancia inferior a diez metros. Su principal uso es para conectar maquinas entre sí. La Figura 4.b hace referencia a redes de área local inalámbricas (WLAN), de este modo existen un conjunto de máquinas capaces de conectarse a un punto fijo (AP) de la red que hace de puente. Estos dispositivos tienen un alcance de unos 100 metros. De este modo el AP controla las transmisiones radio que ocurren dentro de su red. El número de redes WLAN es muy amplio, y está estandarizado en el epígrafe IEEE802.11. Por último, la Figura 4.c identifica las redes celulares, que tienen un área de cobertura muy amplia – típicamente nacional – y se crearon bajo la necesidad de poder utilizar los terminales móviles fuera de casa/oficina, también son conocidas como redes de telefonía móvil.

Dado el indiscutible crecimiento de la telefonía celular durante los últimos años, es lógico tender a un uso de estos terminales, no solo para realizar llamadas telefónicas, sino también para dar acceso a Internet. Las redes celulares nos permiten el acceso inalámbrico a Internet desde cualquier lugar, sin importarnos la limitación de cobertura como en las áreas WiFi [5]. Idealmente este servicio se debería realizar con una velocidad elevada y debería permitir una movilidad lo más transparente posible [6]. Una de las características principales de las redes celulares es la utilización de múltiples transmisiones a baja potencia, con el fin de aumentar la capacidad del sistema con un radio menor. El área de cobertura se divide en celdas, cada una con una antena propia. Estas celdas disponen de una banda de frecuencias asignada y una estación base – transmisor, receptor y unidad de control -. Las celdas contiguas reciben diferentes bandas de frecuencia para evitar problemas de interferencias. La forma típica de las celdas es hexagonal, con el fin de que todas las antenas adyacentes estén equidistantes poder controlar de manera sencilla el movimiento de usuarios y el traspaso de los mismos entre celdas. Como ya se ha mencionado anteriormente, cada celda posee un

sistema de transmisión, donde se controla la potencia de transmisión para permitir la comunicación en la celda usando la frecuencia dada. Típicamente se utilizan de 10 a 15 frecuencias por celda, con el fin de reutilizar estas frecuencias en celdas próximas pero no contiguas, es decir, el diferentes clusters. Como se puede suponer todo este despliegue, mantenimiento y control supone un elevado coste.

Como se ha podido percibir uno de los mayores problemas para las redes celulares es en lo relativo a costes y a frecuencias. Más aun estas últimas, ya que se trata de un recurso natural y limitado. La demanda de este recurso se hace por parte de Administraciones Públicas pero también por parte de empresas privadas, como puede ser operadores de telecomunicación. Al tener una tendencia creciente en cuanto a su demanda es necesario un uso eficiente del mismo, y es necesaria una licencia para su uso por parte del Estado. Estas licencias se otorgan según la legislación vigente de nuestro país por concurso público, abierto y permanente (Artículo 32 de la Ley nº 26522). Uno de los mayores costes que generan las redes celulares son los asociados a infraestructura y cableado, un inconveniente que no posee las redes WiFi [2]. Además estas redes WLAN son aptas para una variedad mayor de dispositivos (móviles, PDAs, portátiles, PCs, notebooks, ebooks, etc.). De igual modo estas redes están siendo utilizadas para dar acceso público a Internet en centros comerciales, estaciones, aeropuertos, etc. El estándar para las redes WLAN es el IEEE802.11, conocido comúnmente como WiFi, que son las redes que vamos a utilizar.

Aunque este estándar contempla también el medio óptico-infrarrojo, debido a la menor cobertura de este, se centra en medio de ondas de radiofrecuencia. Como cabe esperar, este estándar - en función de la modulación, transmisión y tasa de bits - se divide en otros más sencillos [1].

El uso de las WLAN ha aumentado, a la par que su precio ha descendido, su velocidad de transmisión ha crecido y se han ido resolviendo problemas de seguridad en ella [7]. Las organizaciones se han dado cuenta de que son un complemento de las redes cableadas. Las principales ventajas de estas redes son, en primer lugar, que evita el elevado coste de instalación y despliegue de otro tipo de redes. De igual manera, la ampliación de estas redes no supone ningún inconveniente, basta con colocar otro punto de acceso. Están presenten en oficinas, domicilios particulares, cafeterías, aeropuertos, etc. por lo que son, a fecha de hoy, una de las tecnologías más importantes de acceso a Internet [2]. La ventaja más obvia de las redes inalámbricas, y por tanto de la WiFi, es la movilidad. Los usuarios de esta red pueden conectarse a redes ya existentes y desplazarse libremente [7] [3]. Además tienen una gran flexibilidad, lo que puede traducirse en un rápido despliegue. En cuanto a la infraestructura necesaria, es independiente del número de usuarios finales que se vayan a conectar a la estación base. Para aumentar el radio de cobertura de la red simplemente basta con añadir nuevas antenas a la estación.

Los primeros resultados al evaluar las tendencias de consumo de datos han demostrado que el promedio mundial de consumo a través de redes Wi-Fi cuadruplica al de las redes móviles [3]. Para los usuarios, la elección de la red Wi-Fi en su smartphones es una parte importante en cuanto al consumo de datos para poder mantenerse dentro de los límites de su plan de datos. Como se muestra en la Figura 5 el consumo de datos inalámbricos es mayoritariamente debido al tráfico WiFi [3].

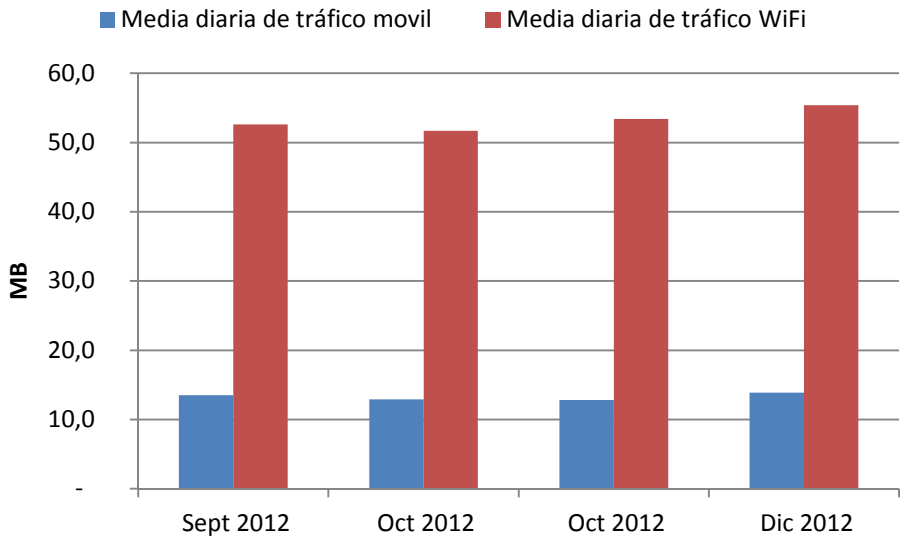


Figura 5 - Detalle uso diario (por usuario) de redes inalámbricas

Conexión con operadores, tráfico Offload.

Por su parte los proveedores de servicios reconocen que el trafico Wi-Fi Offload seguirá creciendo dentro de su planificación de red [3]. Este tráfico consiste en pasar tráfico de redes celulares a otras redes, principalmente WiFi [3], es decir, emplean tecnologías de red complementarias para la entrega de de trafico a redes de datos. Este uso de tecnologías complementarias se puede hacer por parte del usuario final o del operador. Tiene un valor importante para los operadores este tipo de tráfico ya que les permites aliviar su carga de la red de datos, y para los usuarios al poderle ofrecer un mayor ancho de banda al usar tecnologías Wi-Fi.

Gran parte de la actividad de datos se origina dentro de la casa del usuario. Para usuarios con redes Wi-Fi en el hogar una gran proporción de este tráfico se descarga de la red móvil a la red fija, esto se conoce como tráfico Offload. Este tipo de tráfico se espera que aumente al 71% hasta 2017. Con la Figura 6 se refleja que el uso de tráfico Offload va a ser cada vez mayor en los próximos años [3].

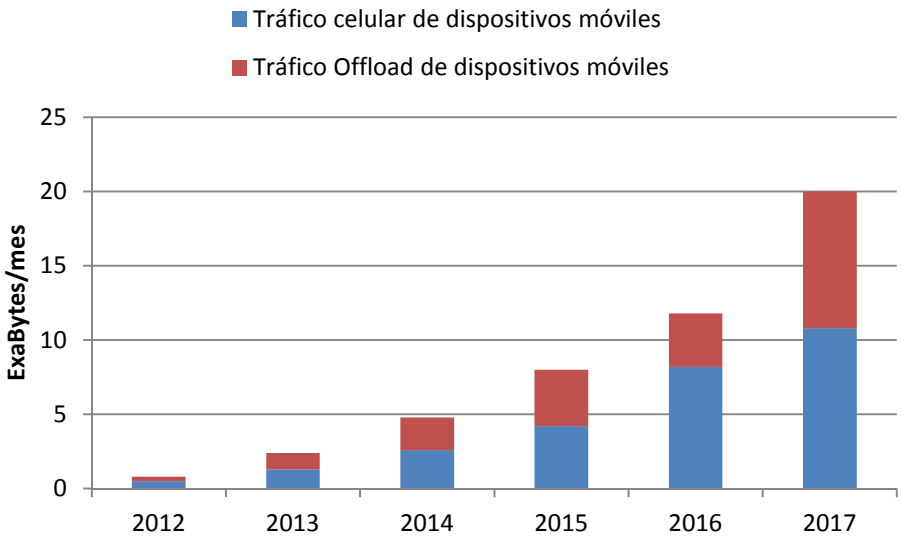


Figura 6 - Utilización de redes por tipo de tráfico

Por todos estos motivos esto se ha optado por hacer un estudio sobre redes WiFi.

2. Monitorización y Mantenimiento

Hasta ahora hemos visto y explicado las diferentes topologías de red inalámbrica y porque pensamos que la WiFi es la que más influencia va a tener en un futuro a medio y corto plazo. Pero llegados a este punto se nos puede plantear la idea de si es necesario llevar un control exhaustivo y detallado de estas redes, más aun cuando transmitimos los datos por el "aire".

Internet es una herramienta crítica para muchas instituciones y muchos ciudadanos confían en Internet para llevar a cabo gran parte de sus gestiones personales y profesionales [8]. Pero detrás de todo esto hay un lado oscuro, en el que pueden atacar nuestra privacidad o incluso volver inoperables algunos servicios. Los principales tipos de ataque que se están detectando son introducciones de software malicioso en hosts [4]. Este software malicioso, o malware, viene junto a archivos que recibimos de Internet, fotos que mandamos, etc. gracias a los cuales existe la posibilidad de que terceros accedan a nuestros dispositivos y los infecten, ya sea para borrar nuestros archivos, instalar software espía, o cualquier otra acción. Los intentos de agresión por medio de malware en el primer trimestre de 2013 alcanzan el 40% de los ordenadores, lo que significa alrededor de 1.300 objetos maliciosos [10]. Debido al incremento de uso de redes inalámbricas esto puede generar una importante vulnerabilidad de seguridad, puesto que se puede examinar y analizar los paquetes que viajan por estas redes sin muchas complicaciones. Simplemente colocando un receptor pasivo en las proximidades de transmisor inalámbrico, recibiendo una copia de todos los paquetes. Estos paquetes pueden contener cualquier tipo de contenido como contraseñas, información confidencial, numero seguridad social, etc. Este

dispositivo es conocido como packet sniffer o analizador de paquetes. Otro ataque típico es la suplantación de identidades, debido a la simplicidad de elaboración de los paquetes con contenido personalizado y su posterior envío por la red, es fácil emitir paquetes con una dirección IP origen falsa, para poder hacerse pasar por otros usuarios. Estos son algunos de los ataques en Internet más comunes, pero existen otros muchos, por ello es necesario llevar un control en la red que garantice su integridad, privacidad y autenticidad [6].

La gestión y mantenimiento son básicos para el buen funcionamiento de una red. Algunos de los fallos que podemos encontrar – y solucionar – gracias a este control son, por ejemplo, la detección de fallos en una tarjeta de interfaz. Aunque es fácil disponer de herramientas para que alguna entidad de la red informe ante fallos en sus interfaces, se puede tener una parte de administración que monitoriza y analiza el tráfico en tiempo real, por la cual sería posible la previsión de dicho problema antes de que ocurra y sustituir la tarjeta, en este caso, antes de que llegue a fallar. Un administrador puede, por ejemplo, ser capaz de realizar comprobaciones periódicas de los host de su red y actuar previo a la caída de alguno de ellos. Gracias a la monitorización de tráfico se puede llegar a la implantación de recursos que faciliten u optimicen el sistema, como detectar enlaces de la red con congestión y que necesiten una ampliación de ancho de banda. De nuevo estos son algunos de los casos prácticos que se pueden llevar a cabo gracias a la monitorización de la red [9].

Para solucionar problemas en 802.11 la mayoría de las veces es necesario un analizador de paquetes para poder analizar a bajo nivel lo que está sucediendo en el protocolo [9]. Los analizadores pueden dar datos sobre la intensidad de la señal, canales utilizados, etc. Las técnicas de monitorización consisten en la captura de tráfico en los distintos canales para reunir información representativa de las tramas de la red. Este enfoque de monitorización, en algunos casos, puede resultar insuficiente debido a que estas redes permiten tráfico en múltiples canales en paralelo, mientras que la monitorización solo se puede realizar en un canal determinado. Por esto es necesario controlar todos los canales, de manera periódica, y obtener trazas de tráfico representativo de cada uno de ellos. Si se detecta alguna anomalía, es necesaria una muestra de tráfico más amplia, o incluso la necesidad de llegar a identificar la ubicación del dispositivo problemático, por lo que será necesario, una vez identificado el fallo, centrar un estudio sobre él [10]. Algunas de las aplicaciones más comunes de estos sistemas son la localización de dispositivos, gracias a esta monitorización y al estudio de los resultados obtenidos es posible localizar/emplazar un dispositivo dentro de un área determinada. También pueden ser útiles para la medición de la calidad de VoIP. En los últimos años estos servicios están creciendo de manera exponencial, lo que permitirá dar un mayor y mejor servicios a los usuarios. Otra aplicación bastante crucial que podemos realizar es controlar la seguridad en la red, nos permite controlar muchos aspectos de la red, desde los usuarios conectados, tipo de mensajes que intercambian, sus identificaciones, etc. [5]

3. Estructura de la Memoria

La memoria se divide en diferentes partes, alguna de ellas a su vez contienen varios capítulos. El contenido de la misma se resume en:

1. **Primera parte: Introducción.** En esta parte se hace una introducción a redes inalámbricas, se explica la estructura de la memoria y las fases de su trabajo. Contiene los siguientes capítulos:

    - Capítulo 1: Redes inalámbricas.
    - Capítulo 2: Monitorización y mantenimiento.
    - Capítulo 3: Estructura de la Memoria.
    - Capítulo 4: Fases de desarrollo.

2. **Segunda parte: Introduction.** En esta parte se hace una introducción a redes inalámbricas, pero en lengua inglesa:

    - Capítulo 5: Wireless Networs.
    - Capítulo 6: Monitoring and management.

3. **Tercera parte: Diseño.** Esta parte se centra en explicar el diseño elegido, los objetivos que se intentan lograr y los requisitos necesarios. Se detalla a mayor nivel la arquitectura diseñada y las herramientas necesarias. Se compone de los siguientes capítulos:

    - Capítulo 7: Objetivos y Requisitos.
    - Capítulo 8: Arquitectura.
    - Capítulo 9: Hardware.
    - Capítulo 10: Software.
    - Capítulo 11: Configuración.

4. **Cuarta parte: Despliegue**. En esta sección se describe el despliegue diseñado y su implementación, tanto a nivel lógico como físico. De igual manera se describen algunas de las aplicaciones del sistema. Consta de los siguientes capítulos.

    - Capítulo 12: Introducción.
    - Capítulo 13: Configuración lógica.
    - Capítulo 14: Despliegue físico.
    - Capítulo 15: Implementación.
    - Capítulo 16: Resultados.

5. **Quinta parte: Conclusiones y trabajos futuros**. En esta parte se explican las conclusiones obtenidas del trabajo realizado así como proyectos futuros que se podrían realizar para complementar el actual. Se compone de un solo capitulo.

6. **Sexta parte: Conclusions and future works**. Se describen las conclusiones obtenidas en lengua inglesa.

4. Fases del desarrollo

El Trabajo Fin de Grado se dividió en las fases de desarrollo siguientes:

- **Documentación y análisis del estado del arte:** Esta primera parte de trabajo se dedicó al estudio y evaluación de las redes inalámbricas actuales, así como a detectar sus principales problemas o inconvenientes para tratar de solucionarlos.

- **Estudio de la infraestructura a desplegar:** En esta parte se plantearon varias alternativas de topologías de red para el estudio del tráfico en redes 802.11.

- **Despliegue de la infraestructura:** Una vez decidida la infraestructura necesaria y planteado el sistema, se pasó a esta parte en la que se desplegó la red por el Departamento para el estudio de su tráfico.

- **Toma de datos:** En esta parte se programaron unos scrpits para obtener los datos del estudio.

- **Evaluación de los resultados:** Con los datos ya obtenidos se analizaron y se obtuvieron las conclusiones pertinentes.

Parte II

Introduction

II. Intoduction

5. Wireless Networks

This document describes the project developed as my Degree Thesis. It designs an infrastructure to analyze the 802.11 traffic and its practical implementation

In recent years the world has become increasingly mobile. So traditional ways of communication networks are not enough to face the new challenges posed by that new way of life. If users have to be connected to the network by cables physically, mobility would be very limited. This is why wireless connectivity is becoming crucial, allowing great freedom of movement to users. For all these, wireless technologies are invading the field of networks.

According to a Cisco's study, has been proved the importance in nowadays society - and future - of wireless technologies. This study shows that the worldwide mobile traffic grew 70% in 2012, reaching the 885 petabytes per month. Also, the traffic almost duplicated last year's values. The average of purchases on smartphones grew 81% in 2012. Globally the 33% of all the traffic is downloaded over Wi-Fi. It is estimated that in the next five years, mobile traffic will reach values higher than 10 exabytes (an increase of thirteen times the current traffic). The number of connected devices will exceed the world's population, and the 50% of the global traffic will be generated with smartphones. It is also estimated that 21 exabytes of data traffic will be downloaded by Wi-Fi networks.

As it is noted in Figure 1, it will be a growing trend of mobile traffic over the next five years. It is estimated that this growth will be worldwide; it is true that in the more developed areas around the world both its growth, and its use, will be even higher, as it is shown in Figure 2. It is also noteworthy that the use of this technology, although it will be more important on smartphones devices, these will not be the only ones suffering such growth, and it will produce a similar increase in the other devices capable to support this technology, as it is shown in Figure 3.

All this, leads us to be in a position to assert that wireless networks will suffer a very important growth process all around the world in the coming years, thanks in part because it is supported by many mobile devices.

Wireless networks, unlike wired ones, do not require a fixed connection to a terminal point of the network, but in this case, communication networks are performed by radio transmissions. The most common use given to wireless networks consists in facilitate user's mobility, not to replace wired networks. (In a short-medium term would be replaced because of wireless networks have many advantages, mainly because of its lower price and their easy deployment in emergency situations. Might involve to replace part of the network backbone with wireless infrastructure). Depending on the use there will be many different types of wireless networks, in Figure 4 they are classified according to their coverage area.

Figure 4.a corresponds to an ad-hoc model, where a device acts as a master and the rest as slaves. The last ones should be connected to the master within a distance of less than ten meters. Its main use consists on connecting machines together. Figure 4.b refers to wireless local area networks (WLAN), in which there is a set of machines capable of connecting to a fixed point (AP) of the network that acts as a bridge. These devices have a range of about 100 meters. Thus the AP controls the radio transmissions occurring within its network. The number of WLAN networks is very broad, and is standardized in section IEEE802.11. Finally, Figure 4c identifies cellular radio networks, which have a very wide coverage area - typically national – and they were created by the necessity of using mobile terminals away from home or the office. These are also known as mobile phone networks.

As the cellular growth is undisputed in recent years, it is logical to tend to use these terminals not only for making phone calls, but also to provide access to the Internet. Cellular networks allow us to access wireless to the Internet from anywhere, no matter the limitation of WiFi coverage areas. Ideally this service should be done with a high speed and mobility should be as transparent as possible. One of the main features of cellular networks is the use of multiple low power transmissions, in order to increase system capacity with a smaller radius. The coverage area is divided into cells, each with its own antenna. These cells have been assigned a frequency band and also a base station - transmitter, receiver and control unit -. The neighboring cells receive different frequency bands to avoid interference problems. The typical shape of the cells is hexagonal, so that all adjacent antennas are equidistant to control easily the user movement and its transferring between cells. As already mentioned above, each cell has a transmission system where the transmission power is controlled to allow communication in the cell using the given frequency. As usual 10 to 15 frequencies are used per cell, and they are reused these neighboring cells but not contiguous. As expected, all this deployment, maintenance and control have a high cost.

One of the biggest problems for cellular networks are frequencies, more than costs, because they are a limited natural resource. The demand for this resource is done by the Government and also by private companies, such as telecommunications operators. Given the upward trend in their demand is necessary an efficient use of them and it requires a State license.

Also one of the biggest costs that cellular networks generate are those concerning to the infrastructure and wiring, a problem that WiFi networks does not have. Besides, these WLAN networks are not suitable for a wide range of devices (phones, PDAs, laptops, PCs, notebooks, ebooks, etc.). Similarly these networks are being used to provide public Internet access at malls, train stations, airports, etc. The standard for WLANs is the IEEE 802.11, commonly known as WiFi, which are the networks that we will use.

Although this standard includes the optical medium, because of the reduced coverage of it, it focuses on radio waves. As expected, this standard is divided into simpler ones.

The use of WLANs has increased, alongside its price has fallen, its transmission rate has increased and some security problems have been solved. Organizations have realized that they are a complement to wired networks. The main advantages of these networks are that avoids the high cost of installation and deployment that have other networks. Similarly, the expansion of these

networks poses no problem, just placing another access point. These networks are present in offices, private homes, cafes, airports, etc. so they are nowadays, one of the most important technologies of the Internet.

The most obvious advantage of wireless networks, and therefore WiFi networks, is mobility. Users of these networks can connect to existing networks and move freely. They also have a lot of flexibility, which can translate into rapid deployment. As for the necessary infrastructure, it is independent of the number of users connected to the base station. To increase the radio network coverage it is necessary just to add new antennas to the station.

First results evaluating data consumption trends have shown that the average of world consumer via Wi-Fi quadruples mobile networks. For users, the choice of Wi-Fi on their smartphones is an important part on the consumption data in order to remain within the limits of their data plan. For their part, service providers recognize that the Wi-Fi Offload traffic will continue growing within their network planning.

For all this we have chosen to do a study on WiFi networks, as it is shown in Figure 5 wireless data consumption is mainly due to WiFi traffic.

It also has great importance, as mentioned above, Offload traffic from the mobile network to the permanent network. This is the use of complementary network technologies to deliver traffic to data networks. This use of complementary technologies can be done by the end user or the operator. It has an important value for operators this kind of traffic because it let them relieve their burden of data network, and also for users to be able to offer more bandwidth to use Wi-Fi technology.

Much of the data activity is originated within the user's home. For users with Wi-Fi networks in their house for a large proportion of this traffic is download from the mobile network to the home network, this is known as traffic offload. This type of traffic is expected to increase to 71% until 2017. Figure 6 shows the growing in the coming years.

6. Monitoring and management

So far we have seen and explained the various wireless network topologies and why we think that WiFi is going to have more influence in the medium and short future. But at this point, we could wonder whether it is necessary to take a comprehensive and detailed control of these networks, even more so when we transmit the data through the "air".

. Internet is an important tool for many institutions and many people rely on the Internet to carry out much of their personal and professional efforts. But behind all this there is a dark side, where can attack our privacy or become inoperable some services. The main types of attacks are being detected are malware introductions in hosts. This malicious software, or malware, comes with files we receive from the Internet, photos we send, etc. through which it is possible for third parties to access and infect our devices, whether to delete our files, install spyware, or anything else. The

aggression attempts by malware in the first quarter of 2013 reached the 40% of computers, which means about 1,300 malicious objects. Due to the increasing use of wireless networks, it can generate important security vulnerability, because we can review and analyze the packets traveling throughout these networks without any complications just placing a passive recipient on the nearness of the wireless transmitter, receiving a copy of all packets. These packages can contain any type of content such as passwords, confidential information, social security number, etc. This device is known as packet sniffer or packet sniffer. Another typical attack is identity spoofing, because of the simplicity of drawing packages with customized content and its later delivery by the network; it is easy to issue packets with a false IP address to impersonate other users. These are some of the most common Internet attacks, but there are many others, so it is necessary to control the network to ensure its integrity, privacy and authenticity.

The management and maintenance are essential for the proper functioning of a network. Some of the faults we can find - and fix - thanks to this control are, for example, the detection of failures in an interface card. Although it is easy to have tools for any network entity to report faults in the interfaces, where can have a part of management that monitors and analyzes traffic in real time which would be possible to predict the problem before occurs and replacing the card, in this case, before it fails. An administrator can, for example, be able to conduct periodic checks of the host on your network and act before the fall of one of them. Thanks to monitoring traffic we can reach the implementation of resources to facilitate or optimize the system such as how to detect network links with congestion and requiring a bandwidth expansion. Again, these are some of the studies that can be carried out by monitoring the network.

To solve 802.11 problems usually we need a packet sniffer to analyze low-level what is happening in the protocol. The analyzers can provide us information of the signal strength, channel used, etc. Monitoring techniques consist in capturing traffic on different channels for gathering information representative of the network frames. Monitoring techniques sometimes can be insufficient due to this networks allow traffic on different channels at the same time, while the monitoring can just been done in a particular channel. Therefore it is necessary to control all channels periodically and obtain representative traffic traces of each one. If an abnormality is detected, we will need a more extensive traffic sample, or even the need to identify the location of the offending device, so it will be necessary once the fault is identified focus a study on it. Some of the most common applications of these systems are locating devices, thanks to this monitoring and to the study of the results is possible to locate / place a device within a certain area. May also be useful for measuring the quality of VoIP (in recent years such services are growing exponentially) which will provide more and better services to users. Another important application is to control the network security, we can control many aspects of the network from users connected, type of messages exchanged, to their identification.

Parte III

Diseño

III. Diseño

En este apartado se va a describir el diseño de la arquitectura propuesta y la configuración a alto nivel del sistema implementado en el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid. Este sistema consta de un nodo central – en este caso un PC – que hace funciones de servidor, y varios nodos inalámbricos desplegados por este Departamento monitorizando la red. De manera auxiliar se realizará un análisis de los resultados para mostrar el funcionamiento del sistema y alguna de sus aplicaciones.

7. Objetivos y Requisitos

En el estudio previo al desarrollo del sistema que se va a implementar se han definido los siguientes objetivos y requisitos que debían ser cumplidos.

Objetivos:

- Despliegue físico de una red inalámbrica en el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid.
- Despliegue de una infraestructura para analizar tráfico 802.11.
- Breve evaluación de los resultados obtenidos para comprobar el correcto funcionamiento del sistema.

Requisitos:

- Nodos capaces de automatizar acciones.
- Nodos sin necesidad de una capacidad de memoria amplia, al guardar información en el servidor.
- Capacidad de procesamiento medio-bajo debido a que gran parte del trabajo se va a desarrollar en nodos inalámbricos no generan demasiada carga.
- Nodos de coste económico por la necesidad de desplegar un gran número de ellos.
- Nodos con acceso a red cableada.
- Ordenador para realizar funciones de Servidor.
- Servidor con elevada capacidad de procesamiento y capacidad de compresión de archivos.

8. Arquitectura

La arquitectura desplegada para la realización de este Trabajo Fin de Grado ha sido la siguiente.

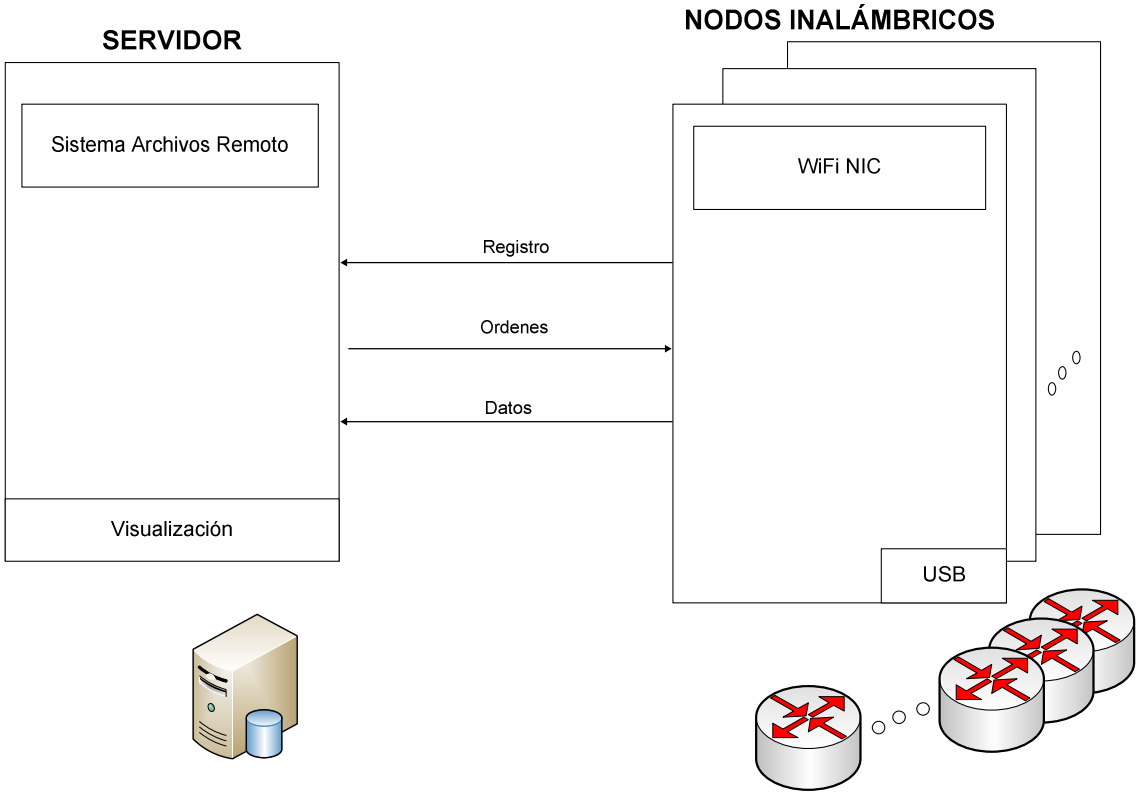


Figura 7 - Arquitectura del sistema

Como se puede ver en el diagrama de la Figura 7 se ha optado por una arquitectura formada por un servidor y varios nodos inalámbricos - en particular routers Fonera - que trabajan en paralelo.

El servidor es el elemento central de la red, puesto que se encarga de recoger el tráfico capturado por el resto de nodos. De manera auxiliar se realiza un breve análisis y procesado para finalmente ser presentarlo al usuario. Para almacenar los datos los nodos disponen de un sistema de archivos remoto que crean en el servidor.

Por su parte los nodos inalámbricos que han sido utilizados han sido Fonera 2.0n, tienen como elemento base una interfaz Wi-Fi y de manera auxiliar un dispositivo de almacenamiento con memoria flash, por si fuese necesaria más memoria.

El mecanismo de funcionamiento consiste en un registro por parte del nodo inalámbrico en el Servidor. Una vez se ha realizado este proceso correctamente, el servidor le manda una serie de

acciones u órdenes a realizar a cada nodo. Los nodos una vez han completado dichas órdenes, guardan la información en el servidor para que se puedan analizar con el fin de administrar la red de modo eficiente.

9. Hardware

El hardware que ha sido necesario para la realización de este proyecto ha sido:

- **Servido**r: PC ubicado en el laboratorio 4.1.F04 del Departamento de Ingeniería Telemática, con las especificaciones detalladas en la Tabla 1

Nombre	Babosa
Kernel	2.6.32-5-amd64
Distribución	GNU/Linux Debian 6.0
Procesador	Intel Core Quad (2.66GHz)
RAM	4GB
Wireless	No

Tabla 1 - Especificaciones servidor

- **Nodos inalámbricos**: Tras un estudio del mercado sobre los diferentes routers disponibles se ha optado por Fonera 2.0n debido a su bajo coste y elevada flexibilidad [11]. Sus especificaciones son las mostradas en la Tabla 2:

Nombre	Fonera 2.0n
CPU	Ralink 300MHz
RAM	64MB
Flash	8MB
Puertos Ethernet	1 WAN (10/100MB)+ 4 LAN (10/100MB)
USB	USB 2.0/1.1 (Ralink)
WiFi	Ralink RT3052
Alcance WiFi	40-200m
Descarga-Subida simultánea	Si
Dimensiones	30mmx157mmx127mm
Antenas	2 x 3 dBi Dipolos
Autenticación	WEP,WPA,WPA2,WPA mixta
Estándares de red soportados	IEEE802.11g/b/n

Tabla 2 - Especificaciones nodos inalámbricos

- **Dispositivos de almacenamiento externo**: Se ha optado por el uso de pendrives por su bajo coste y tamaño compacto. Con estas características detalladas en la Tabla 3:

Nombre	Kingston
Capacidad	4GB
Interfaz	USB 2.0
Velocidad Lectura	10 MB/s
Velocidad Escritura	5MB/s

Tabla 3 - Especificaciones dispositivos almacenamiento externo

10. Software

Para el apartado de software han sido necesarias las siguientes herramientas:

- Distribución para los nodos: **OpenWrt**

OpenWrt es una distribución de firmware libre basado en GNU/Linux altamente extensible a estos dispositivos [11]. Se ha elegido esta distribución por estar construida desde la base, facilitando su funcionalidad, lo que lo convierte en una herramienta fácilmente modificable, altamente beneficioso para el nodo ya que cuenta con unas capacidades limitadas. El proyecto OpenWrt comenzó en 2004 y empezó a dar soporte a múltiples dispositivos. Proporciona un sistema de archivos completamente modificable con gestión de los paquetes, y no un único firmware estático. Lo que nos libera de la configuración proporcionada por el proveedor y nos permite personalizar el dispositivo de manera manual.

Aunque se ha optado por esta distribución se estudió la posibilidad de instalación de otras como Claro OS o m0n0wall, pero fueron descartadas al tener menos capacidades que OpenWrt.

- Sistema Operativo para servidor: **GNU/Linux**.

Nos ofrece una serie de posibilidades que otras – como Windows - no lo hacen, como puede ser la posibilidad de personalizar completamente la máquina, una elevada robustez del sistema, un software libre y tiene un diseño más óptimo para uso redes. Por uniformidad de sistemas operativos también se ha optado por usarlo en el servidor.

- Sistema archivos remoto: **SSHFS.**

Por la arquitectura del sistema era necesario que los nodos tuvieran acceso a ciertos directorios del servidor, además de almacenar información en él, por eso se optó por un sistema de archivos virtual [13]. Un mecanismo muy sencillo y bastante completo que nos permite hacer esto -

y que cumple con los requisitos de del sistema a desarrollar – que está optimizado para sistemas Linux (que usamos en ambos extremos) es el sistema SSHFS, que cuenta con una implementación FUSE.

Aunque en un primer lugar se pensó en realizar la monitorización guardando los datos en una memoria flash. Esta opción fue descartada por suponer un esfuerzo innecesario en los nodos, ya que era necesario una carga de trabajo muy elevada al tener que estar comprimiendo los datos (acción que debido al limitado procesador podría llegar a saturar los nodos) y enviándolos al servidor, así como por un estudio realizado en el que se comparaban – porcentualmente – el número de paquetes capturados en cada uno de los modelos frente al número de paquetes enviados. Para la elaboración de este estudio se realizó de manera controlada envío de tráfico entre diferentes dispositivos con varios nodos capturando dicho tráfico y almacenándolo en remoto gracias a SSHFS, o en local – en pendrives o discos duros-. Los resultados contenidos en la Figura 8 muestran un mayor porcentaje de paquetes capturados, o lo que es lo mismo, una mayor eficiencia al realizar las capturas, por SSHFS. Cada uno de los test consta de 5 pruebas de medida en diversas situaciones.

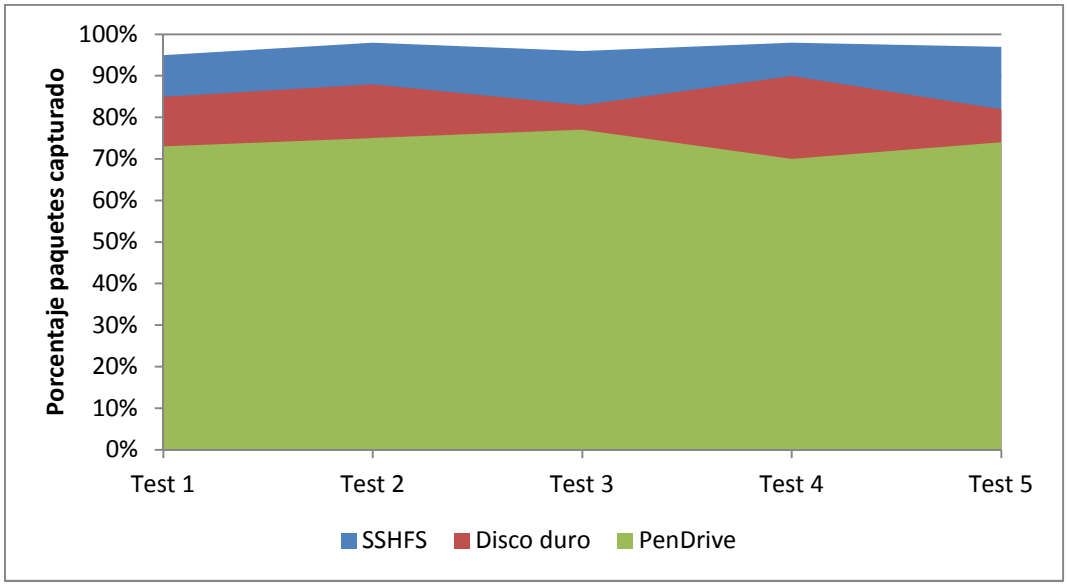


Figura 8 - Comparativa paquetes capturados

Han sido descartados otros sistemas al tener más limitaciones que SSHFS, como Gmail FS, que guarda los datos como correos en una cuenta de Gmail, o GlusterFS. Por su parte SSHFS trabaja a través de SSH utilizando un entorno seguro de acceso. Gracias a ello el cliente puede interactuar libremente con el sistema montado en el servidor.

- Analizador de tráfico: **TCPDUMP**.

Una de las bases del proyecto es la captura y análisis del tráfico de la red. Esta herramienta cumple con las necesidades y es de uso fácil gracias a que se trabaja sobre línea de comandos [14]. Nos permite capturar, mostrar o guardar los paquetes que circulan por la red, e incluso realizar análisis en tiempo real.

Por el sistema operativo elegido han sido descartados otros analizadores como WinDump, que son para Windows. Además de otros para Linux como tshark[1] [15] no soportado por los nodos.

- Sincronización: **NTP**.

Debido a la necesidad de estar recogiendo datos en varios nodos, era necesario que la información recogida estuviese bien sincronizada, para, a la hora de analizarlos, poder compararlos de manera coherente según el momento en el que fueron recogidos.

El mecanismo más sencillo es NTP o Network Time Protocol. Es un protocolo de Internet a nivel de aplicación, que sincroniza los relojes de los sistemas según la escala de tiempo UTC[2] [15]. Es el protocolo mayormente utilizado en Internet.

- Visualización resultados: **Highcharts**.

Destacar que la visualización no es el objetivo de este proyecto, simplemente se ha desarrollado una herramienta de visualización en tiempo real para mostrar algunas de las aplicaciones prácticas del sistema desplegado.

Para la representación y análisis visual de los resultados se ha optado por la herramienta Highcharts [16]. Esta es una biblioteca de gráficos escritos en HTML5[3] y javascript, de modo que ofrece al usuario una interacción con la aplicación web muy intuitiva. Los modos de visualización son muy amplios desde líneas, diagramas de barras, burbujas, etc.

Se ha tomado la decisión de usar esta herramienta por su versatilidad a la hora de trabajar con los distintos navegadores, funcionando prácticamente en todas las versiones de cada uno de ellos. Una característica importante es que, si su uso es sin ánimo de lucro o personal, no se necesitan permisos para su publicación en nuestras webs. Además de poder descargar el código fuente y poder editarlo según las necesidades de la aplicación, gracias a su sintaxis de configuración sencilla. Es una herramienta muy práctica para la representación de datos a tiempo real debido a la completa API de la que dispone en combinación con librerías como jQuery.

[1] Tshark es un analizador de protocolos de red. Es capaz de capturar paquetes de una red a tiempo real, de leer paquetes ya capturados o incluso mostrar cierta información de estos.
[2] UTC corresponde a las siglas *Universal Time Coordinated*, es el principal estándar de tiempo encargado de gestionar los relojes del mundo.
[3] HTML5 es la quinta revisión del lenguaje de programación HTML. Especifica variantes de sintaxis para HTML.

- **Análisis matemático: MATLAB**

Nuevamente incidir en que esta no es la finalidad del Trabajo Fin de Grado, si no que se ha realizado de manera auxiliar para ver sus usos y capacidades.

Para el análisis de los datos de necesitaba un software matemático para optimizar los cálculos. Uno de los más extendidos – usado frecuentemente a lo largo de la carrera en la universidad – es MATLAB. Está disponible para múltiples plataformas y su uso es sencillo e intuitivo.

11. Configuración

El servidor es el elemento principal del sistema, y se encargará de las siguientes funciones:

- Llevar un registro de los nodos activos con algunas de sus capacidades y características principales.
- Coordina las funciones a desarrollar por los nodos inalámbricos.
- Almacena la información recogida por los nodos.
- Analiza y representa la información recogida.

Los nodos inalámbricos son parte crucial en el sistema, encargados principalmente de capturar tráfico de la red. Como se aprecia en la Figura 7, el sistema se divide en tres fases. En la primera de ellas los nodos inalámbricos están encargados de realizar un registro en el servidor indicando algunas de sus capacidades; una segunda fase en la que el servidor indica las órdenes o acciones que cada nodo en particular deben realizar; y la última fase en la que los datos obtenidos por los nodos son almacenados en el servidor.

Parte IV

Despliegue

IV. Despliegue

12. Introducción

En esta sección se describe el despliegue realizado para la realización del proyecto.

Dicho despliegue ha sido realizado en el Departamento de Ingeniería Telemática de la Universidad Carlos II de Madrid, por algunos de sus laboratorios y despachos. En el departamento existen dos subredes, la 163.117.139.0/24 y la 163.117.140.0/24. Los nodos inalámbricos al contar con DHCP[4], pueden obtener direcciones de cualquiera de las dos subredes. Para el acceso local a los nodos se creó una subred, la 10.7.23.0/24, asignando direcciones a puertos de los nodos y poder conectarse directamente a ellos en caso de fallo y reconfigurarlos de manera local.

13. Configuración lógica

Al contar el Departamento de dos subredes diferentes como son la 163.117.139.0/24 y la 163.117.140.0/24 los nodos inalámbricos al, obtener una dirección IP por DHCP, pueden coger una IP de cualquiera de las dos subredes. De modo que, previo a su despliegue, se configuró en una de sus puertos de red una IP estática para poder acceder en local a ellas y corregir posibles fallos. Dicho rango de IP estáticas pertenecen a la subred 10.7.23.0/24. Esta subred también sirvió para configurar inicialmente los nodos desde el servidor. El servidor pertenece a uno de las subredes de Departamento y tiene asignado en una de sus interfaces una IP estática.

La distribución a nivel lógica está definida en la Figura 9.

[4] DHCP es un protocolo de red que permita a los usuarios de una red IP obtener su configuración automáticamente.

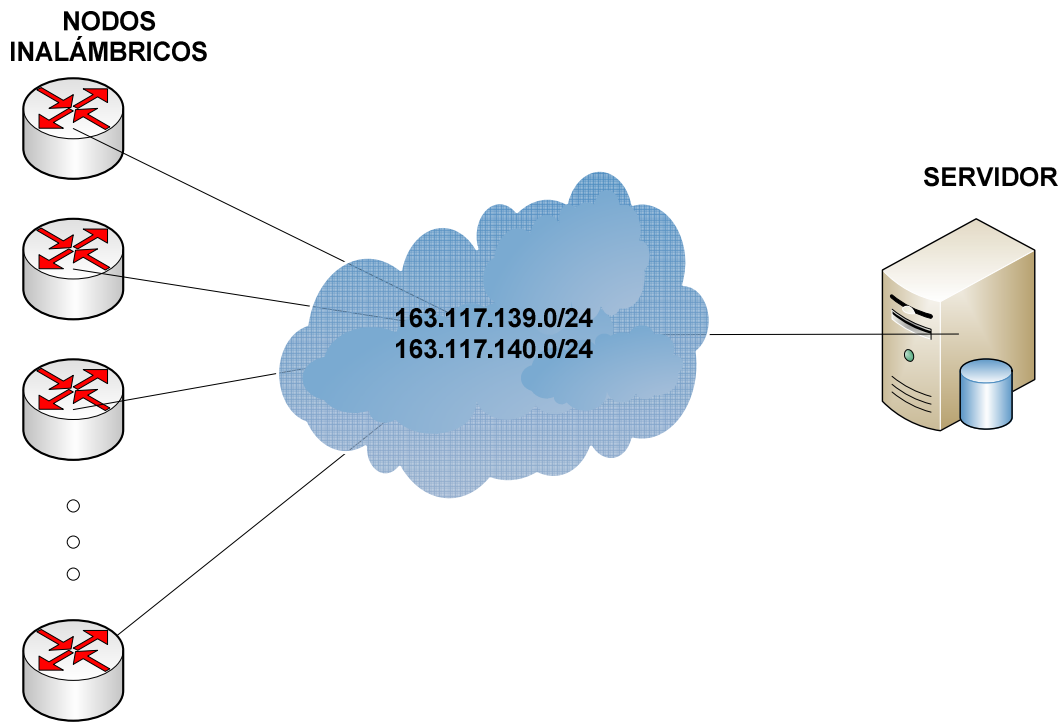


Figura 9 – Configuración lógica del sistema

14. Despliegue físico

En esta sección se va a describir la arquitectura del sistema a nivel físico.

El servidor está localizado en el laboratorio 4.1.F04 del Departamento. Aula habilitada dentro del Departamento de Ingeniería Telemática para el desarrollo de Trabajos Fin de Grado por su buena accesibilidad dentro del área del Departamento.

Se desplegaron un total de 11 nodos inalámbricos por todo el Departamento de Ingeniería Telemática, dejando en backup otros 3 para utilizarlos en caso de fallo. Su distribución en los diferentes laboratorios se detalla en la Tabla 4:

Fon1	4.1.A03
Fon2	4.1.F13
Fon3	4.1.A03
Fon4	4.1.C01
Fon5	4.1.A14
Fon6	4.1.F01
Fon7	4.1.F15
Fon8	4.1.F03
Fon9	4.1.F03
Fon10	4.1.A16
Fon11	4.1.C01

Tabla 4 - Localización nodos inalámbricos

En la Figura 10 se puede apreciar dicha distribución sobre la planta del Departamento, indicando con puntos rojos la localización de los nodos.

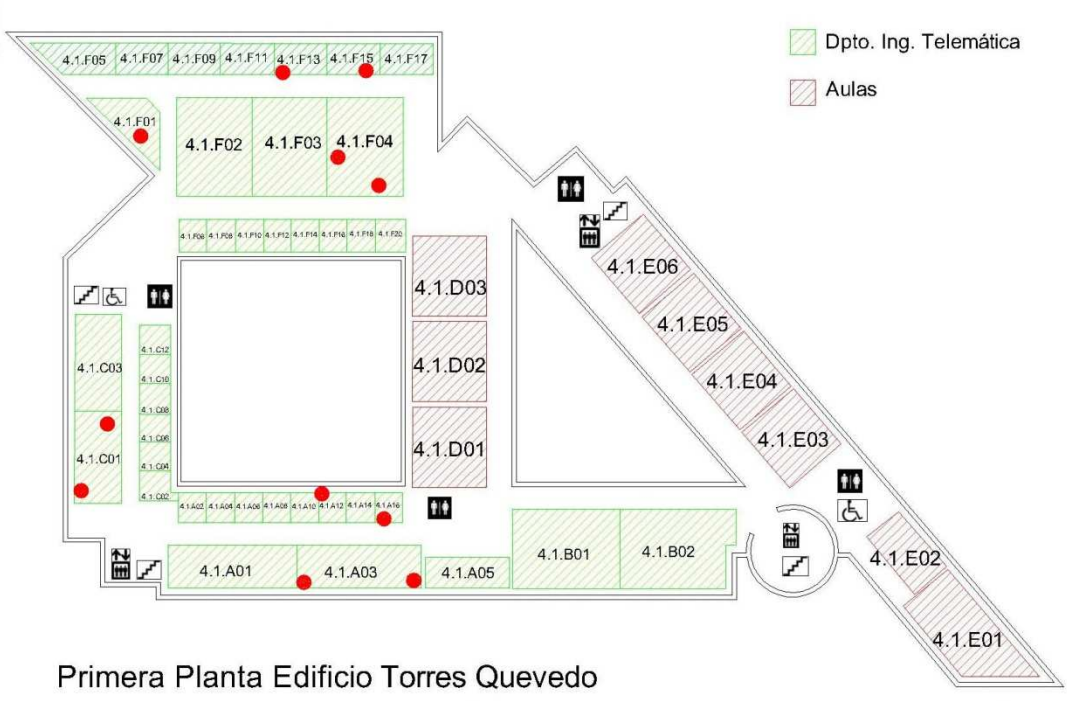


Figura 10 - Arquitectura de diseño a nivel físico

15. Implementación

En esta sección se va a explicar el proceso seguido para el diseño del sistema. De manera adicional, se ha diseñado alguna de las múltiples aplicaciones que se pueden llevar a cabo gracias a la arquitectura y diseño realizado, para comprobar su funcionamiento y utilidad.

15.1. Servidor

En primer lugar, se ha configurado en el servidor un directorio específico para la realización del Trabajo Fin de Grado. Este contiene todo el material necesario para la implementación del sistema diseñado. Consta básicamente de un directorio que sirve de nexo con los nodos inalámbricos, gracias al sistema de archivos remotos, SSHFS y la obtención de una pareja de claves pública/privada. Este directorio está detallado en la Figura 10. Como se puede apreciar su contenido son otros cuatro directorios: Registro, Órdenes, Capturas y Análisis. Esta pareja de claves nos permite realizar una autenticación de manera transparente, es decir, sin necesidad de introducir una contraseña manualmente. El mecanismo consiste en generar una pareja de claves

publica/privada en la maquina que hace de cliente, gracias al protocolos SSH[5], y al otro extremo se le indica la clave pública del cliente al cual deseamos dejar acceder con la clave privada asociada.

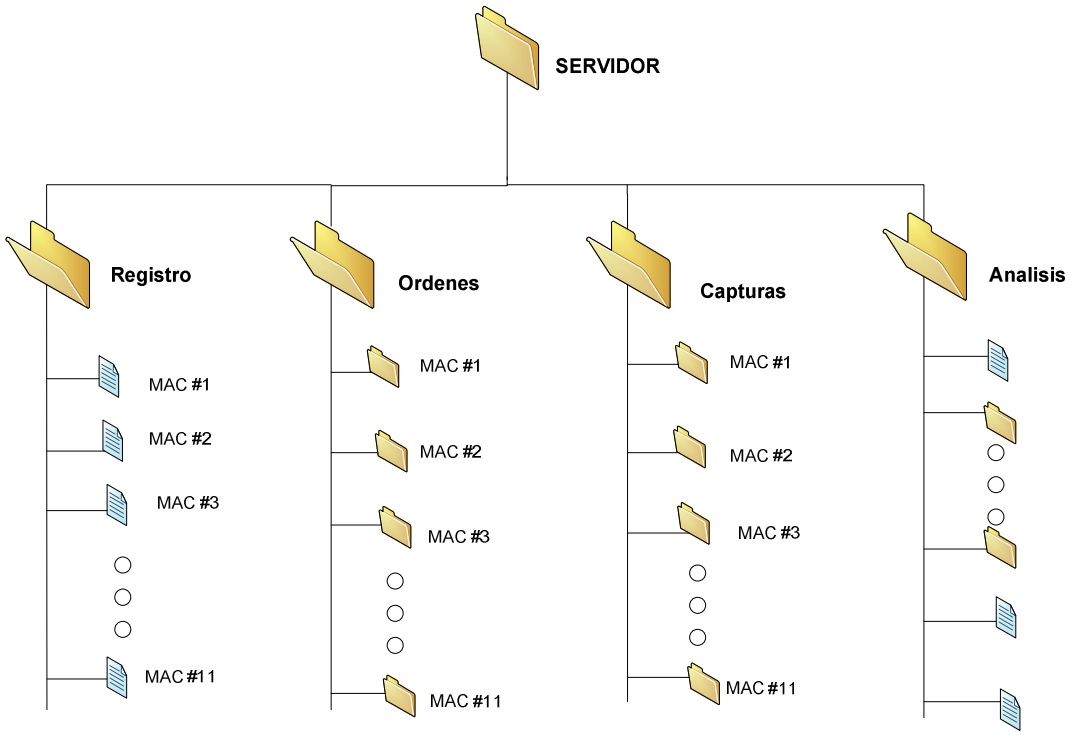


Figura 11 - Diseño servidor alto nivel

El directorio de *Registro* cuenta con un archivo de texto por nodo inalámbrico, creado y editado por los mismos nodos, en los que se almacena la dirección IP que han obtenido los nodos por DHCP perteneciente a las subredes del Departamento, así como si poseen capacidad de almacenamiento externo o no. El nombre de estos archivos coincide con la dirección MAC[6] de cada nodo. Por su parte el directorio *Órdenes* contiene a su vez un directorio propio para cada nodo inalámbrico. En él se le especifica al nodo, por parte del usuario (ya que para la implementación del sistema la parte del servidor carece de inteligencia) las acciones que debe realizar cada nodo una vez que ha sido registrado. Estas acciones son de dos tipos: permanentes, es decir, que las va a estar realizando continuamente en segundo plano; y las no permanentes, estas órdenes se leen y realizan de manera periódica por si sufren cambios. En el directorio de *Capturas*, como en Órdenes, existe un subdirectorio especifico para cada nodo inalámbrico, identificando cada uno de ellos por la dirección MAC del nodo al que están asociados. En estos directorios se almacenan las capturas de tráfico de la red realizadas por los nodos, que son las principales ordenes que van a recibir. Por último en el directorio de *Análisis* se realizan todos los cálculos y estimaciones necesarias para el estudio y representación de los datos obtenidos.

[5] SSH se define así al protocolo y nombre que lo implementa utilizado para acceder a máquinas remotas a través de una red

[6] Dirección MAC es un identificador que está asociado de forma única a una tarjeta de red.

Como herramienta auxiliar, en paralelo, en el servidor se ha creado una aplicación web de visualización (gracias a Highcharts) corriendo en el puerto 3000 del servidor, que sirve para mostrar al usuario los datos que se estimen, en este caso se trabajará con throughput asociados a los nodos, que se puede observar en la Figura 12 .

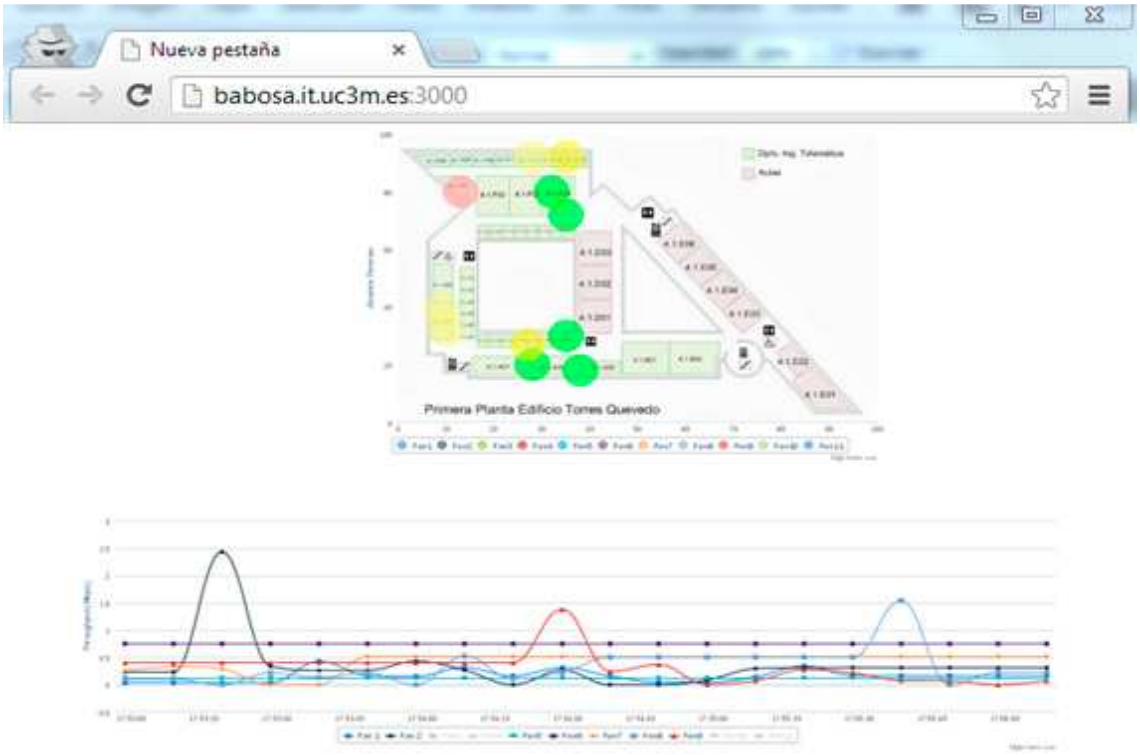


Figura 12 - Aplicación

15.2. Nodos inalámbricos

En los nodos inalámbricos se ha llevado a cabo una configuración más en detalle. En primer lugar se ha instalado un firmware OpenWrt, como se detalla en el Apéndice 2 del Anexo, para poder trabajar de manera más sencilla con ellos. Una vez actualizados los nodos se ha pasado a realizar los cambios necesarios para satisfacer las necesidades de la aplicación. Los procesos de configuración para el sistema que realizan los nodos se detallada en Figura 13.

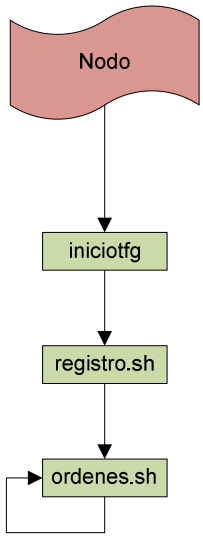


Figura 13 - Procesos realizados por los nodos inalámbricos

15.2.1. Al iniciar el nodo

En primer lugar en el directorio */etc/init.d*, en el cual se especifican todas las acciones que deben ser realizadas por los nodos al iniciarse, se ha creado otro script, en este caso llamado *inifiotfg*. Este documento se encarga de, en primera instancia, obtener las credenciales necesarias para poder conectarse al servidor sin necesidad de introducir ninguna contraseña, y posteriormente llama a un script ubicado en */etc/archivos/registro* (directorio creado específicamente para el sistema) que se encarga de registrar a los nodos en el directorio creado para tal fin en el servidor.

15.2.2. Registro en el servidor

El script llamado desde *iniciotfg* que realiza las operaciones de registro en el servidor se nombra como *registro.sh*, sus funciones son: en primer lugar obtener su dirección MAC y guardarla en distintas variables – y en diferentes formatos - para operar posteriormente con ellas, en segundo lugar obtener su dirección IP perteneciente a una de las dos subredes del Departamento e identificar si posee o no, en ese momento, capacidad de almacenamiento en dispositivo externo – identificando como 0 si no la posee, y 1 en caso de que sí - . Estos dos valores son escritos en un fichero de texto y enviados al servidor para formalizar el proceso de registro. Uno de las acciones más importantes que realiza este script es la creación del sistema de archivos remoto creado por SSHFS con el servidor. La asociación se va a crear entre el directorio */mnt/babosa* – creado para realizar esta asociación fin en cada nodo - y un subdirectorio dentro del directorio *Capturas* del servidor. Para realizar estas operaciones y no necesitar introducir credenciales - con el fin de automatizar el proceso - se hace uso de la librería SSH que nos permite realizar estas operaciones, indicando el lugar donde se ha guardado el par de claves pública/privada comentadas anteriormente [17]. Este script finaliza con la llamada a otro, éste encargado de realizar las acciones que el servidor estime oportunas, en este caso dicho script se llama *ordenes.sh* y está ubicado en */etc/archivos/ordenes/*.

15.2.3. Acciones a realizar

Este script, *ordenes.sh* es el que tiene mayor carga en el nodo. Sus funciones son, en primer lugar (y como el script anterior) obtener su dirección MAC. Posteriormente se descarga desde el directorio *Órdenes* del servidor, el contenido del subdirectorio asociado a su MAC, para obtener las acciones que el servidor estima que debe realizar. Estas acciones van a ser principalmente trabajo de monitorización de la red que se puede divide en tres fases. Se muestra todo el proceso en la Figura 14.

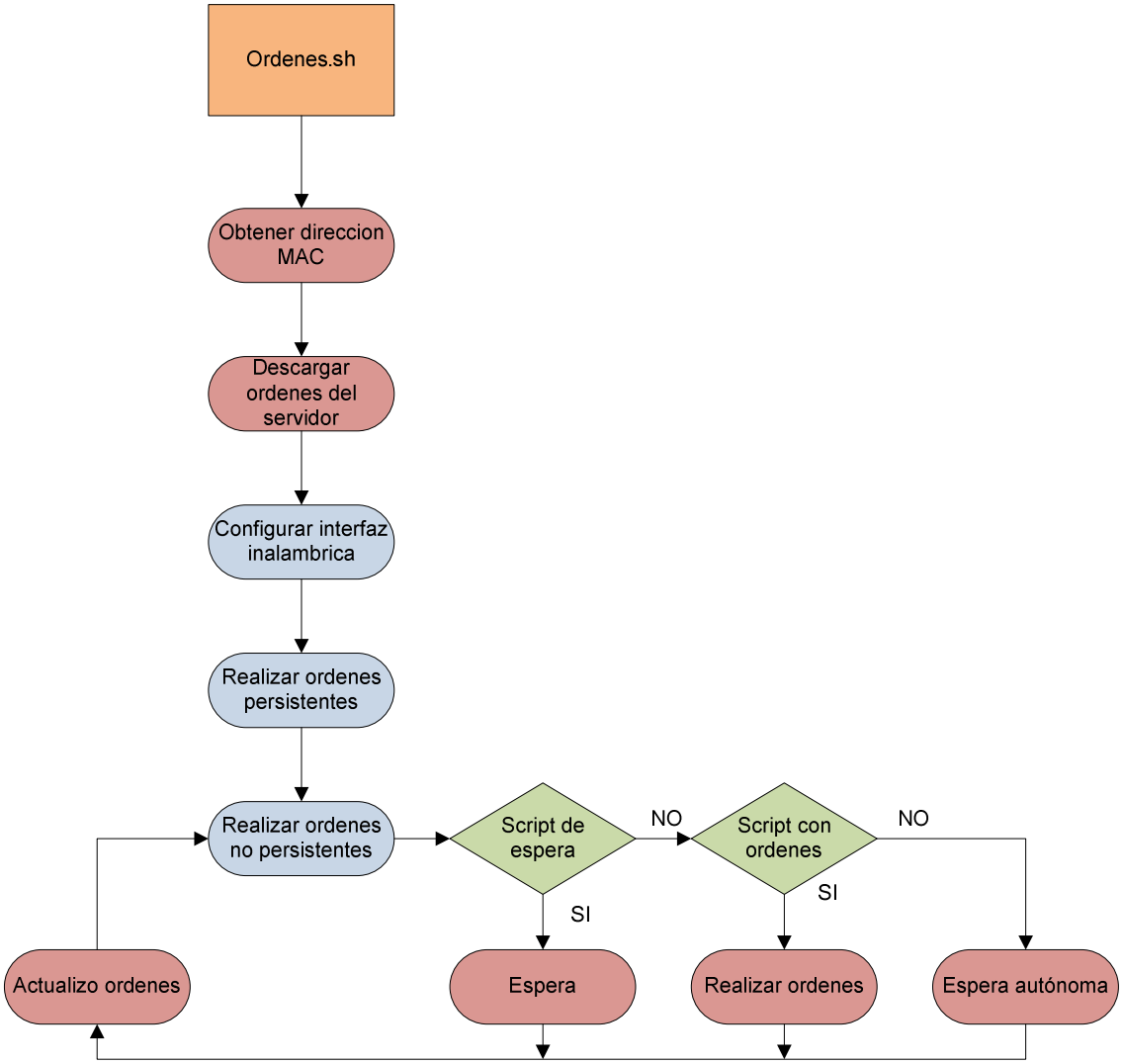


Figura 14 - Diagrama script ordenes.sh

La *primera fase* consiste en configurar la interfaz inalámbrica mediante el script *scriptWireless.sh*. Gracias a este script se puede configurar manualmente cualquier parámetro de la interfaz que queramos modificar, en nuestro caso los valores que van a ser cambiados típicamente van a ser el canal y el punto de acceso al que debe conectarse - si así se estima oportuno- . Finalmente se habilita una interfaz en modo monitor. Las ventajas de este tipo de interfaz es que trabaja en modo pasivo, es decir que no transmite ningún tipo de tráfico [17], y además permite monitorizar todo el tráfico recibido por su tarjeta de red inalámbrica, sin necesidad de estar

conectado explícitamente a ninguna red. Una *segunda fase* en la se descarga un script desde el servidor y es ejecutado, si es que existe, con el fin de realizar las órdenes persistentes que ha de realizar, este script recibe el nombre de *script_persistant.sh*. Estas son las que se estarán realizando en segundo plano permanentemente en el nodo. Típicamente van a ser acciones de captura de tráfico, se le indicará además un valor de frecuencia, que nos indica el periodo de duración de cada captura de tráfico con la herramienta TCPDUMP. Se realizan capturas, por ejemplo, cada 30 segundos y se almacenan en el directorio temporal. Con esto se obtiene una monitorización continua de la red en la que se encuentran los nodos, para su posterior análisis en el lado del servidor. La *tercera fase* de las órdenes, que va a recibir el nodo inalámbrico, consiste en un bucle en el que se actualiza periódicamente las acciones que el servidor manda a cada nodo inalámbrico. Estas órdenes pueden ser de dos tipos: de espera, en el que solo se especifica el periodo de inactividad al nodo, de órdenes determinadas a realizar (en el caso excepcional de que el servidor no mande ninguna orden al nodo, este pasará a un periodo de inactividad de forma autónoma).Estas acciones a realizar se reciben mediante los scripts *script_espera.sh* y *scriptX.sh* respectivamente,

15.2.4. Evaluación

Una vez configurado todo el sistema el mecanismo normal de actuación es mandar a los nodos periódicamente diferentes acciones de monitorización. Llevado a cabo, gracias al script *scriptX.sh* ubicado en el subdirectorio asociado a cada nodo en el servidor y descargado por los nodos. El contenido de este fichero, es decir, las acciones u órdenes que se han llevado a cabo para probar en correcto funcionamiento del sistema se detallan en la Figura 15 y se explican en los párrafos siguientes.

La primera acción que realiza el script es obtener su dirección MAC, como se venía haciendo en anteriores scripts, para poder identificarse en el servidor y poder almacenar las capturas en él. Como se describió en partes anteriores de la memoria, los nodos inalámbricos carecen de una capacidad de almacenamiento interna muy elevada, por lo que se ha optado por un almacenamiento periódicamente de las capturas de tráfico realizadas por los nodos en un directorio en el servidor, aunque previamente hayan sido guardadas en local en cada nodo. Se han definido varios temporizadores para realizar las operaciones de monitorización. Un primer temporizador que define el tiempo que se va a estar calculando el throughput de la red (para la parte de aplicación principalmente), *timer_media*; otro que define la frecuencia de cambio de canal – al circular el tráfico en la red por diferentes canales, *timer_cambio_canal*. Se ha optado por hacer la monitorización por los canales más cargados (que típicamente que son el canal 1, 6, 11 y 13) y así tener una muestra representativa del tráfico total de la red - ; un tercer temporizador para pasar las capturas de tráfico del nodo al servidor, *timer_envio_datos* – para no saturar la conexión nodo-servidor en una primera instancia se guardan las capturas en local de manera temporal y periódicamente se pasan al servidor - ; por último existe un temporizador para indicarle al servidor que debe comprimir las capturas que se le ha ido pasando, con el fin de optimizar la memoria y el rendimiento del servidor, *timer_compresion*.

Después de la obtención de estos temporizadores y variables, se entra en bucle, hasta alcanzar el valor de compresión definido por su temporizador, en el que se realizan tres tipos de acciones diferentes. La primera acción se realiza cuando se alcanza el temporizador de cálculo de

medias, en este caso, se almacena en un directorio del servidor el throughput medio de la red en ese intervalo – además de las coordenadas geográficas relativas al Departamento, que tienen almacenados los nodos- , estos datos se recoge principalmente para la parte de aplicación, para la visualización del tráfico en tiempo real. La segunda acción que se lleva a cabo dentro del bucle -que se realiza si se alcanza el temporizador de cambio de canal- es realizar un cambio de canal de manera aleatoria entre los canales 1, 6, 11, 13 que son los que llevan típicamente una mayor carga de tráfico por ser los más usados habitualmente. La última de las acciones es almacenar en el servidor las capturas de tráfico que se están haciendo en segundo plano y de manera persistente en el nodo. Esta operación se realiza al alcanzar el temporizador correspondiente, al estar pasando las capturas al servidor de manera periódica se evita congestionar la conexión entre el nodo y el servidor, que se produciría si se almacenasen los datos directamente en el servidor. Por último este script se encarga de indicar al servidor – ya que como se ha mencionado anteriormente carece de inteligencia -, que debe comprimir los datos que le han sido pasados, de este modo se ahorra memoria en el servidor, y se agrupan las capturas pertenecientes al intervalo de tiempo definido.

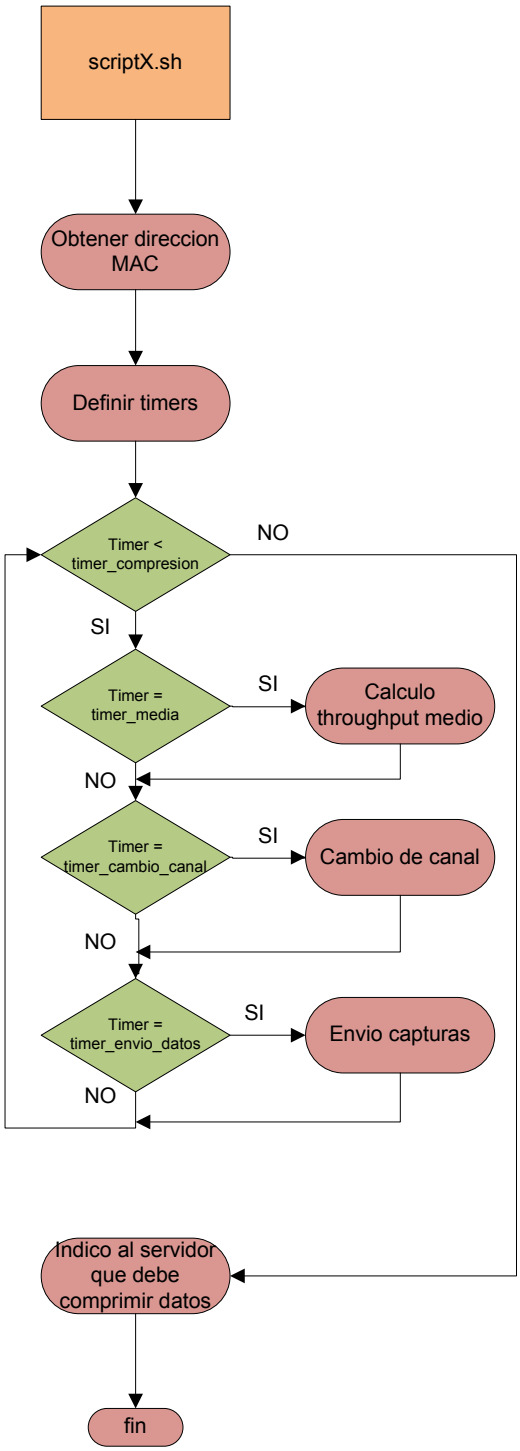


Figura 15 - Diagrama scriptX.sh

15.3. Aplicación

Una vez comprobado el correcto funcionamiento del sistema y con la finalidad de ser además de práctico y útil, fácil de manejar para el usuario se ha desarrollado de manera extra

herramientas de análisis de los resultados. Se ha creado una aplicación web basada en programación HTML. Para poder desarrollarla se ha hecho uso de sockets [19] (para mandar información al navegador) – y de Highcharts, una librería escrita en javascript que nos facilita la creación de gráficas. A modo de ejemplo, de entre los distintos tipos de resultados que podemos visualizar gracias a esta herramienta, se ha optado por representar una figura con la localización de los nodos por el Departamento con una escala de valores en función de la carga de red que monitorizan. Y por otro lado se muestra un gráfico con el throughput que están capturando de la red. Estas dos figuras se actualizan en tiempo real gracias a los sockets. Otros métodos que se han descrito para mostrar información han sido mapas de gradiente y graficas de carga.

16. Resultados

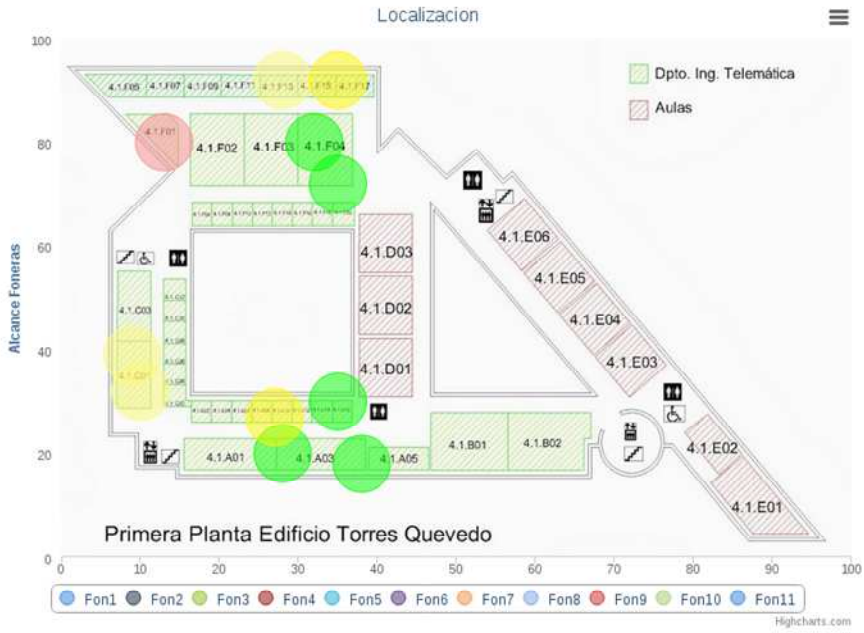
Los resultados obtenidos han sido más que satisfactorios. Por un lado tanto los nodos inalámbricos como el servidor han cumplido con los requerimientos del sistema y han tenido un comportamiento durante la realización de este Trabajo Fin de Grado sin fallo alguno. Por otro lado ya se dispone de datos de la red durante un periodo amplio de tiempo como para hacer estudios sobre la red.

Aunque no era el objetico principal de este Trabajo Fin de Grado, se ha realizado un análisis de los datos obtenidos gracias a la monitorización realizada. Se ha centrado en tres enfoques diferentes. El primero de ellos, ya mencionado, es la visualización en tiempo real en la aplicación web; también se han realizados mapas de gradiente en función de la carga monitorizada por los nodos en el Departamento; y por último la generación de gráficas que muestran el throughput soportado, detallado para el intervalo de tiempo deseado.

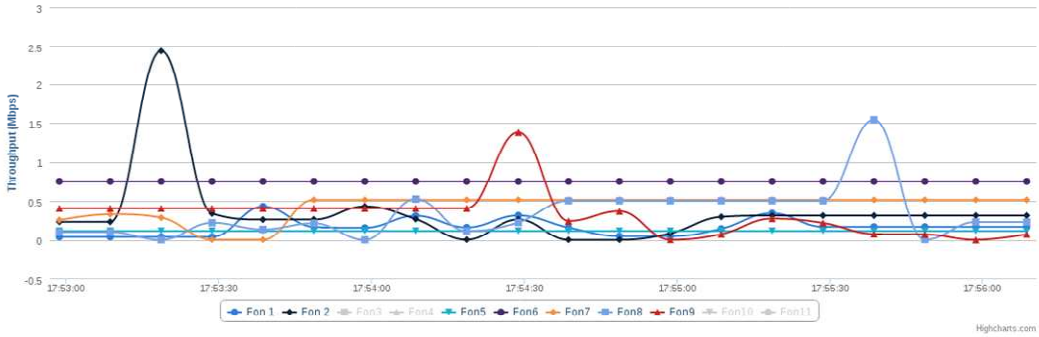
16.1. Visualización en tiempo real

A parte de estar monitorizando y guardando las capturas en el servidor para poder analizar y gestionar de modo eficiente la red (en caso de posibles errores o fallos a posteriori de la monitorización), se ha creído interesante ofrecer al usuario una herramienta de visualización de los resultados en tiempo real.

Con el sistema diseñado y desplegado en el Departamento se ha podido representar, a través de los datos recogidos en tiempo real diversa información. Los nodos inalámbricos distribuidos por el Departamento de Ingeniería Telemática, como se ha descrito anteriormente, están monitorizando la red. A tiempo real, en función del temporizador que definamos en el servidor para realizar los cálculos, se almacenan en el servido las coordenadas geográficas de localización relativas al plano del Departamento y el throughput que es capturado por los nodos en dicho intervalo. Mediante la aplicación web desarrollada se representa esta información en dos formatos distintos como muestra la Figura 16.



(a)



(b)

Figura 16 - Detalle visualización

La Figura 16.a muestra sobre un plano del Departamento el emplazamiento de los nodos. Como se puede observar existe una escala de colores a la hora de representar cada nodo. Esta escala de color está asociada a una de valores, esta vinculación se representa en la Tabla 5. Para definir los umbrales se ha hecho un estudio del throughput medio visto en la red durante varias semanas, se ha comprobado que estadísticamente el 90% de las veces no se superaban los 600KBps, por lo que se ha optado por este como umbral superior. Se observa de manera intuitiva que los nodos de color más intenso representan una carga mayor en la red, y que estos valores varían a lo largo del día.

Color	Valor
Verde claro	Throughput ε (0 , 100) KB/s
Verde oscuro	Throughput ε (100 , 250) KB/s
Amarillo claro	Throughput ε (250 , 400) KB/s
Amarillo oscuro	Throughput ε (400 , 600) KB/s
Rojo	Throughput > 600 KB/s

Tabla 5 - Asociación valores-colores

La Figura 16.b representa, a modo de gráfica, el throughput visto por los nodos. Se muestra en detalle este valor a la vez que se actualiza el mapa anterior, para poder comparar en caso de que fuera necesario detalles de alguno de ellos.

16.2. Mapas de gradiente

Otra aplicación llevada a cabo gracias al sistema realizado ha sido la representación de áreas de carga de aquellas zonas del Departamento por las que han sido desplegados los nodos. Se ha tomado la información que se tenía, es decir la que los nodos estás recogiendo y almacenando en el servidor, y se ha extrapolado al resto de de zonas sin información del Departamento. Esto nos ha llevado a obtener unos mapas de gradiente en los que se ha superpuesto el plano del Departamento para identificar más cómodamente las distintas zonas, como nos muestra la Figura 17.

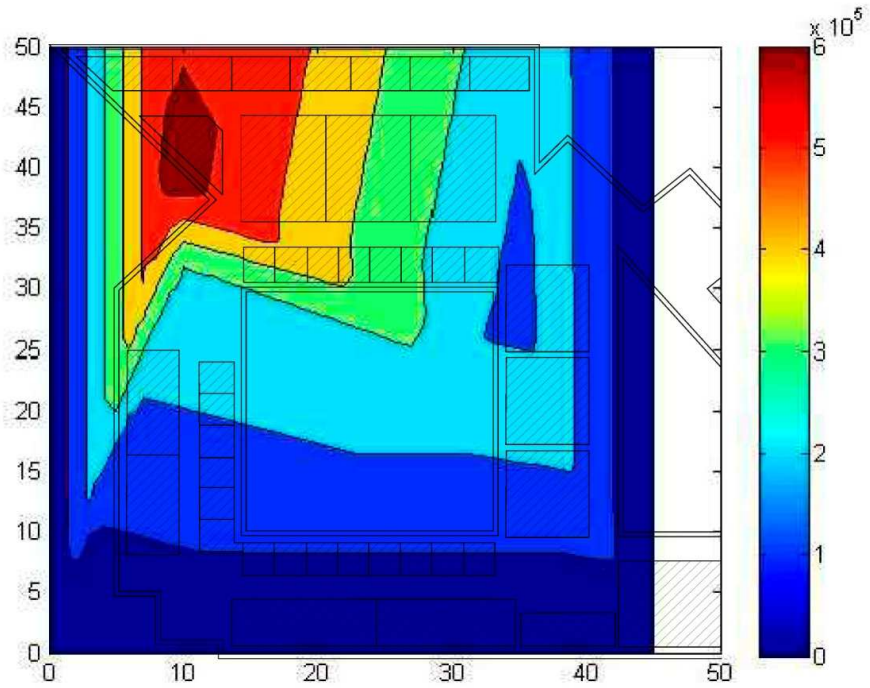


Figura 17 – Detalle mapas gradiente (Kbps)

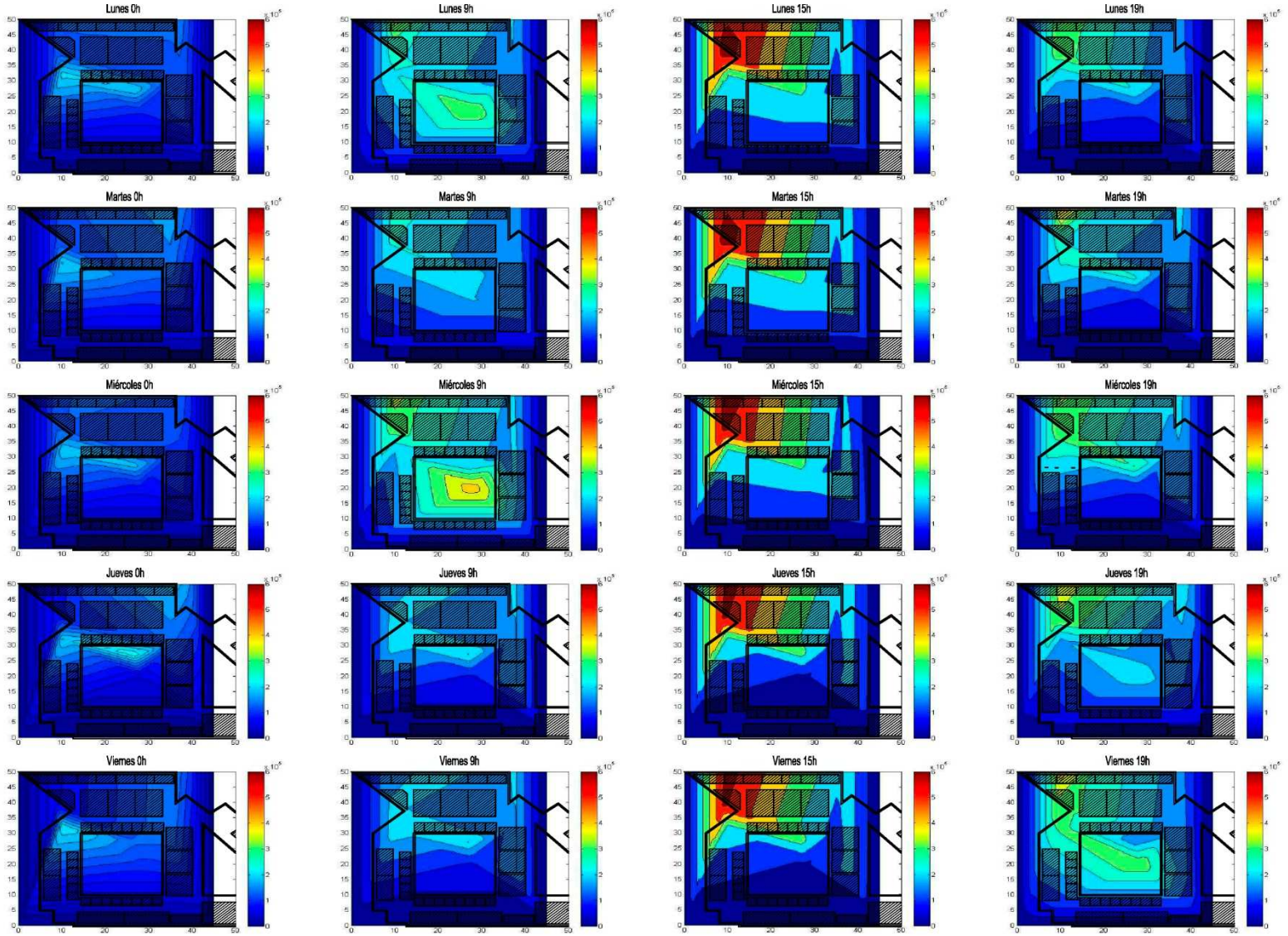


Figura 18 - Mapas gradientes semanal (Kbps)

En un estudio más detallado con estos tipos de mapa, como los de la Figura 18 podemos ver la evolución de la red durante una semana. Se representa el throughput visto en la red a lo largo de una semana. Las filas detallan el día de la semana, de lunes a viernes, mientras que las columnas representan cuarto horas representativas a lo largo del día. Se ha optado por representar valores con diferentes cargas en la red, las horas elegidas han sido las 0 horas, las 9 horas, las 15 horas y las 19 horas. Esta herramienta resulta muy útil para además de monitorizar la red poder hacer una administración más optima. Con los datos obtenidos se pone de manifiesto que durante la tarde-noche la congestión de la red no es elevada (colores azules), mientras que a medio día se puede apreciar una congestión en la zona superior izquierda del Departamento (colores rojizos). Del mismo modo se observa que el uso de la red es bastante uniforme a lo largo de la semana, en la misma franja horaria.

Con estos resultados se podrían llevar a cabo diferentes operaciones para la optimización de la red. Algunas de las sugerencias que se proponen son una mejor distribución de los puntos de acceso, ya que se observa zonas con una diferencia de carga bastante significativa en la misma franja horaria. Otra solución podría pasar por inhabilitar determinados puntos de acceso por la noche, al no tener prácticamente carga la red. Una posibilidad más es la instalación de nuevos puntos de acceso en las zonas con colores más intensos, pues la carga que soportan es mayor. Además de las sugerencias de administración de la red, esta herramienta también es útil para, por ejemplo, ver zonas sin cobertura de la red, picos puntuales de carga, etc.

16.3. Graficas de carga de la red

Una manera distinta de interpretar los datos ha sido mediante gráficas en las que se muestra el throughput de la red. En esta ocasión se han tomado muestras representativas de cuarto de los nodos inalámbricos situados en el Departamento, elegidos de manera uniforme en lo referente a su localización, para tener muestras representativas de todas las áreas, se muestra su localización sobre el plano del Departamento en la Figura 19. La identificación y elección de los nodos se detalla en la Tabla 6

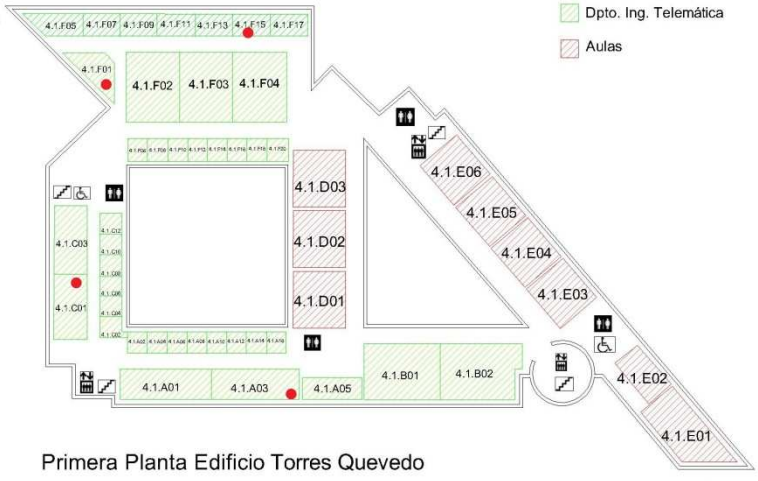


Figura 19 - Distribución nodos para estudio sobre gráficas

Identificador	Localización
Nodo #1	4.1.A03
Nodo #2	4.1.F01
Nodo #3	4.1.F15
Nodo #4	4.1.C01

Tabla 6 - Localización nodos para estudio sobre gráficas

En la Figura 20 se muestra el detalle a lo largo de una semana. Gracias a esta herramienta podemos determinar que el tráfico a lo largo de la semana es periódico, con esto se quiere decir que todos los días de la semana (a excepción del fin de semana que se produce una disminución) se obtienen graficas con el mismo patrón. Esto es, un primer pico entorno a las 10-12 am, y un segundo pico menor entorno a las 14-16 horas. También se observa que la carga soportada por los distintos nodos, es decir, por las diferentes zonas del Departamento siguen el mismo patrón, aunque la carga neta en heterogénea.

Con esta herramienta se pueden apreciar picos de tráfico en la red e identificar el intervalo de tiempo en el que se produjeron, para poder controlar la red. Se puede ver si la distribución de carga en las diferentes zonas del Departamento se distribuye de manera homogénea, que hemos visto que no es el caso. Indicativo de que se podrían llevar a cabo procesos de optimización en la red, como por ejemplo, ampliar el número de puntos de acceso en las zonas próximas a los nodos que observan una mayor carga.

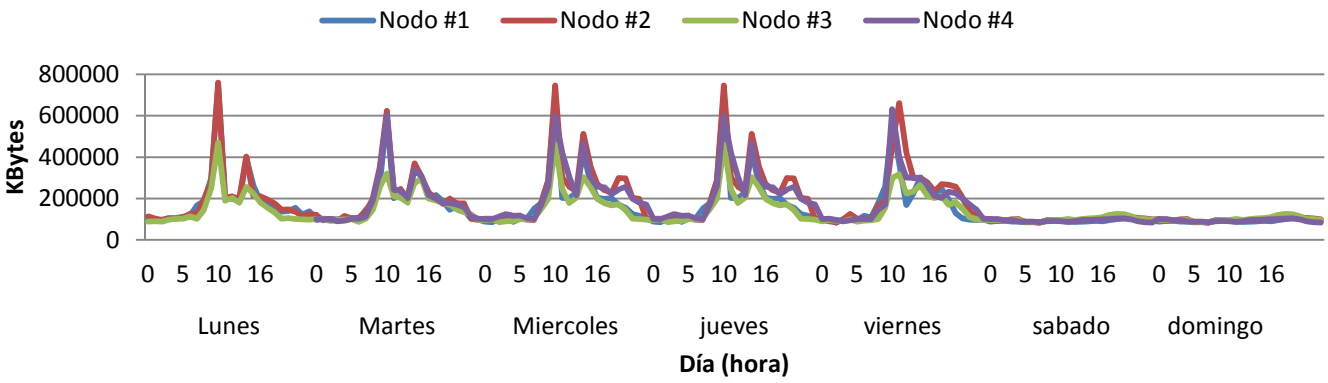


Figura 20 - Graficas carga semana vista por nodos

Parte V

Conclusiones y trabajos futuros

V. Conclusiones y trabajos futuros

1. Conclusiones

El objetivo de este Trabajo Fin de Grado ha consistido en el diseño de un sistema de monitorización para el análisis del tráfico 802.11. Para este estudio se ha desplegado una red por el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid que monitoriza el tráfico WiFi. Además, de forma complementaria, se han realizado distintos análisis de estos datos para mostrar aplicaciones prácticas del sistema desarrollado.

El primer paso para el desarrollo del sistema fue configurar los nodos y el servidor para automatizar las tareas de monitorización de la red del Departamento. Esta automatización se ha llevado a cabo en 3 procesos, el primero de ellos en el que los nodos se registran en el servidor con sus características principales, el segundo en el que el servidor manda a cada nodo registrado las ordenes que deba realizar y finalmente cada nodo guarda en el servidor los datos. Para el despliegue de la red se ha necesitado un servidor – que controla los nodos -, y 14 nodos inalámbricos para monitorizar el tráfico de la red – de los cuales 11 han sido desplegados y 3 se han quedado en backup para caso de fallo de los anteriores-.

Se optaron por Foneras 2.0n como nodos a utilizar en el sistema. Se instaló un firmware más práctico para la posterior configuración de los nodos, el firmware elegido fue OpenWrt y se actualizó a su versión de kernel más actualizada la 3.3.8. Se realizaron pruebas de monitorización con estos nodos y se vio que eran más eficientes si se realizaban las capturas de tráfico en memorias no flash, por lo que se montó el sistema de ficheros remoto para guardar los datos en el servidor. Una vez comprobado el correcto funcionamiento se pasó a configurar lo scripts de automatización de tareas, parte que se desarrolló con éxito. Realizaban las tareas de registro en el servidor, monitorización de la red por órdenes mandadas desde el servidor y almacenamiento de esos datos en el servidor de manera correcta.

En paralelo a lo anterior, en el servidor se creó el directorio y sistema de archivos necesario para la realización de las tareas sin problema alguno. Un pequeño inconveniente que se encontró, a la hora de automatizar las acciones, era el requerimiento por ambas parte de contraseñas al acceder en remoto al otro extremo de la conexión, pero se solventó intercambiando la pareja de claves publica/privada entre nodos y servidor.

Una vez comprobado el correcto funcionamiento del sistema se pasó a desplegar los nodos por el Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid. Se instalaron físicamente 11 nodos distribuidos uniformemente por el Departamento, para monitorizar la mayor cantidad de tráfico representativo de la red. Con dicho fin, la monitorización se realizó entre los canales de mayor ocupación de manera aleatoria.

Desplegado ya el sistema, y comprobado su funcionamiento, se dejaron los nodos inalámbricos monitorizando la red durante casi dos meses. En paralelo a esta monitorización, y con el fin de mostrar algunas aplicaciones prácticas del sistema creado, se realizaron tareas de

visualización y análisis de los resultados. Se creó una aplicación web de visualización de datos en tiempo real – herramienta muy práctica y sencilla de utilizar -, se realizaron mapas de gradientes con el tráfico de la red, y se mostró mediante graficas la carga de red vista por los nodos.

Con los resultados obtenidos se comprobó que el sistema cumple de manera más que satisfactoria con los requisitos que se plantearon, y que puede ser una buena herramienta para gestionar y administrar la red muy eficiente.

2. Trabajos futuros

Se ha visto que es una herramienta muy práctica y que tiene muchas aplicaciones, gracias a ello existen diferentes líneas de trabajo que se pueden seguir en base al sistema diseñado.

La primera mejora que se podría llevar a cabo sería ampliar la infraestructura de la red. Se podría hacer de manera muy sencilla simplemente configurando más nodos y desplegarlos, este despliegue se podría continuar por el Departamento o aumentar el área de estudio.

Otro cambio que se podría implementar era dotar de más inteligencia al sistema. Esta inteligencia se podría llevar a cabo en la parte de los nodos o del servidor. Una aplicación útil que se podría hacer con esta inteligencia es hacer un cambio de canal en la monitorización más eficiente, de modo que se capture en los canales con más tráfico, por ejemplo. También se podría indicar a los nodos que en el proceso de registro deben almacenar una información determinada.

Gracias a esta herramienta de análisis se podrá llegar a gestionar la red en busca de fallos o identificar las zonas o puntos de acceso con mayor congestión para realizar ampliaciones, por ejemplo. De igual modo, relacionado con la administración de la red, se podrían hacer mecanismos de búsqueda de intrusos en una determinada red, o ver los ataques que está sufriendo la red.

Con este sistema, gracias a la monitorización de toda la red, se pueden hacer estudios de uso de la red. Estos estudios se podrían centrar en identificar el uso en las diferentes franjas horarias del día, asociar a cada usuario el uso que le da a la red, etc. Con el sistema diseñado se podría llegar incluso a identificar los usuarios dentro de una red.

Estas son algunas de las múltiples aplicaciones y trabajos futuros que se pueden desempeñar gracias al sistema montado en este Trabajo Fin de Grado.

Parte VI

Conclusions and future works

VI. Conclusions and future Works

1. Conclusions

The aim of this Bachelor Thesis has been to design a monitoring system to analyze 802.11 traffic. A network has been deployed on the Telematics Department of the University Carlos III of Madrid to monitor the traffic. Complementary to this project, various analysis have been done to show that this system works appropriately.

The first step in the development of the system consists on configuring the server and the nodes to automate the tasks of network monitoring on the Department. This automation is carried out in 3 steps. In the first one, the nodes are registered on the server with their main features, in the second one the server sends to each node orders to be executed and finally each node stores the data in the server. For the network deployment it has been necessary a server - which controls the nodes -, and 14 wireless nodes to monitor network traffic – from which 11 have been deployed and 3 of them have been reserved as a backup in case of fail.

Fonera 2.0n has been chosen to be used as wireless nodes in the system. A new firmware was installed in the nodes. With this new firmware the configuration of the nodes has been smoother. The chosen firmware was OpenWrt and it has been updated to its latest kernel version (3.3.8). Some test have been done to prove the monitoring of the network, and they have revealed that capturing traffic in flash memory is not a good way, because many paquets are losing in the monitoring, so it has been decided to mount remote file system to store data. Once the system has been checked the scripts to automate the work are configured, this part was successfully developed. The nodes have been registered y the server, then the server sends orders to the nodes to monitor the network, and then that information is stored in the server.

At the same time in the server it has been created a directory and a file system necessary to make the monitoring without problems. A small problem was found when we had to connect to the other side of the communication, it was required to introduce the password, but it was solved by creating the public/private keys in nodes and server, and they are exchanged.

After verifying the correct operation of the system, it was time to distribute the nodes on the Telematics Department of the University Carlos III of Madrid. 11 nodes were installed, distributed homogeneously on the Department to monitor a representative part of the network traffic. The monitoring was made over the most occupied channels randomly.

Once the system was deployed and its operation verified, wireless nodes allowed to monitor the network for nearly two months. In parallel to this monitoring, and in order to show some practical applications of the created system, some visualization and analysis methods of the results was created. We create a web application displaying data in real-time, network traffic gradient maps, and graphics that show the network load view by the nodes.

With the results obtained in all this process, it works so fine and, can be a good tool to manage a network very efficiently.

2. Future works

It has been seen that it is a very practical tool and it has many uses. There exist different lines to work with the system designed.

The first improvement that could be done would be to expand the network infrastructure. It could be done very easily, simply by configuring more nodes and distribute them. That distribution could be done on this Department or even in other areas.

Another change that could be implemented is to provide more intelligence to the system. This intelligence could be carried out in the part of the nodes or in the server. A useful application that could be done with this intelligence is to make the channel switching more efficient capturing in the busiest channels, for example.

With this visualization tool we can manage the network to find failures or to identify congestion, for example. Similarly, related to the network administration, it could be easy to make intruders searching mechanisms or detect the attacks to the network.

With this system, by monitoring the entire network, we could make a research of the uses of the network. These studies could focus on identifying the use of the network during the day, each associated users with the use that they give to the network, etc.. With the designed system could even lead to identify users in a network.

These are some of the many applications and future work that can be performed through the system created on this Bachelor Thesis.

Parte VII

Anexos

VII. Anexos

A. Planificación de tareas y presupuesto

A.1 Descomposición de tareas

En esta sección se va a descomponer la relación de tareas llevadas a cabo para la realización de este Trabajo Fin de Grado.

Se procede a describir cada una de las tareas dividiendo en las subtareas que se han descompuesto.

- **Tarea A: Documentación y análisis del estado del arte.**
  - **Subtarea A.1: Estudio y análisis de redes inalámbricas**
    - **Descripción**: Se realiza un estudio de las distintas redes inalámbricas que existen.
    - **Objetivos**: Conocer las redes inalámbricas disponibles y elegir la más interesante.
    - **Duración**: 2 semanas.
    - **Recursos**: Ingeniero – 0.5 ingeniero/mes.
    - **Otros**: Tarea inicial del proyecto.
  - **Subtarea A.2: Estudio sobre monitorización y gestión de redes.**
    - **Descripción**: Se estudian los diferentes modos de gestión y monitorización y su utilidad en la actualidad.
    - **Objetivos**: Obtener conocimientos sobre monitorización y administración de redes y su aplicación práctica.
    - **Duración**: 2 semanas.
    - **Recursos**: Ingeniero –0.5ingeniero/mes.
    - **Otros**: Ultima tarea bloque A.

- **Tarea B : Despliegue red inalámbrica**
  - **Subtarea B.1: Estudio de los nodos inalámbricos, Fonera 2.0n**.
    - **Descripción**: Se realiza un estudio sobre el equipo disponible, para la elección de aquel que más se aproxime a las necesidades.
    - **Objetivos**: Conocer las capacidades de los de los nodos y servidor.
    - **Duración**: 2 semanas.
    - **Recursos**: Ingeniero - 0.5 ingeniero/mes.
    - **Otros**: Tarea inicial bloque B.
  - **Subtarea B.2: Actualización nodos inalámbricos**
    - **Descripción**: Se instala el nuevo firmware en los nodos. Probando el correcto funcionamiento en uno de ellos en primer lugar.

- **Objetivos**: Obtener un mayor rendimiento y facilidad de uso en los nodos inalámbricos.
- **Duración**: 3 semanas.
- **Recursos**: Ingeniero – 0.75 ingenieros/mes
- **Otros**: Posterior a B.1

- **Subtarea B.3: Configurar software en equipamiento**
  - **Descripción**: Instalación de todos los paquetes, drivers, etc. tanto en los nodos como en el servidor.
  - **Objetivos**: Tener todo el equipo necesario configurado correctamente para su despliegue y puesta en funcionamiento.
  - **Duración**: 2 semanas.
  - **Recursos**: Ingeniero – 1 ingeniero/mes.
  - **Otros**: Posterior a B.2
- **Subtarea B.4 : Diseño de la red**
  - **Descripción**: Se realiza todo el diseño de la red, a nivel lógico y físico, se asigna el direccionamiento necesario.
  - **Objetivos**: Diseñar el sistema con las direcciones IP estáticas.
  - **Duración**: 4 semanas
  - **Recursos**: Ingeniero – 0.5 ingenieros/mes
  - **Otros**: Posterior a B.3
- **Subtarea B.5: Estudio herramientas visualización**
  - **Descripción**: Se realiza un estudio de todas las herramientas disponibles para la visualización y comprobación del correcto funcionamiento del sistema.
  - **Objetivos**: Mostrar aplicaciones prácticas del sistema diseñado mediante alguna herramienta.
  - **Duración**: 4 semanas
  - **Recursos**: Ingeniero – 1 Ingeniero/mes
  - **Otros**: Posterior a B.6
- **Subtarea B.6: Despliegue físico de los nodos.**
  - **Descripción**: Se colocan los nodos en laboratorios y despachos para tener distribución geográficamente homogénea. Instalando todo el cableado necesario.
  - **Objetivos**: Desplegar la red para monitorizar el sistema
  - **Duración**: 2 semanas.
  - **Recursos**: Ingeniero – 1 ingeniero/mes.
  - **Otros**: Última subtarea de bloque B.

- **Tarea C: Obtención datos.**
  - **Subtarea C.1: Configurar servidor**
    - **Descripción**: Configurar las acciones que debe el servidor mandar hacer a los nodos.
    - **Objetivos**: Automatizar la toma de acciones por parte de los nodos
    - **Duración**: 2 semanas.
    - **Recursos**: Ingeniero – 0.5 ingeniero/mes.
    - **Otros**: Tarea inicial bloque C
  - **Subtarea C.2: Configurar nodos**
    - **Descripción**: Configurar las acciones y scrpits que deben ejecutar los nodos al iniciarse.
    - **Objetivos**: Automatizar las acciones a desarrollar por los nodos al conectarse a una red y encenderse.
    - **Duración**: 2 semanas.
    - **Recursos**: Ingeniero –0.5ingeniero/mes.
    - **Otros**: Posterior a bloque B
  - **Subtarea C.3: Puesta en funcionamiento del sistema y obtención de datos.**
    - **Descripción**: Poner en práctica el sistema diseñado y obtener datos de la red.
    - **Objetivos**: Obtener datos de tráfico en la red del Departamento de Ingeniería Telemática de la Universidad Carlos III de Madrid.
    - **Duración**: 4 semanas.
    - **Recursos**: Ingeniero –1 ingeniero/mes.
    - **Otros**: Posterior a C.2.

- **Tarea D: Análisis de resultados.**
  - **Subtarea D.1: Visualización de resultados en tiempo real**
    - **Descripción**: Implementar herramientas de visualización online.
    - **Objetivos**: Poder ver datos de la red en tiempo real.
    - **Duración**: 3 semanas.
    - **Recursos**: Ingeniero – 0.5 ingeniero/mes.
    - **Otros**: Tarea inicial bloque D, en paralelo con C.3
  - **Subtarea D.2: Mapas de gradiente**
    - **Descripción**: Realización mapas de gradiente con resultados obtenidos
    - **Objetivos**: Mostrar una de las aplicaciones del sistema
    - **Duración**: 1 semana.
    - **Recursos**: Ingeniero –0.25ingeniero/mes.
    - **Otros**: Posterior a C.2
  - **Subtarea D.3: Graficas carga**
    - **Descripción**: Realización de graficas de carga de los nodos con los datos guardados.
    - **Objetivos**: Mostrar otra aplicación del sistema.
    - **Duración**: 1 semana.

        - **Recursos**: Ingeniero –0.25 ingeniero/mes.
        - **Otros**: Posterior a C.2.
- **Tarea E: Memoria**
    - **Subtarea E.1: Organización y estructura de la memoria.**
        - **Descripción**: Se organiza la memoria así como su estructuración.
        - **Objetivos**: Organizar y estructurar la memoria.
        - **Duración**: 1 semanas.
        - **Recursos**: Ingeniero – 0.25 ingeniero/mes.
        - **Otros**: Tarea inicial E

    - **Subtarea E.2: Redacción de la memoria**
        - **Descripción**: Se pasa a redactar la memoria
        - **Objetivos**: Redactar el documento con la estructura definida.
        - **Duración**: 4 semana.
        - **Recursos**: Ingeniero –1 ingeniero/mes.
        - **Otros**: Posterior a E.1
    - **Subtarea E.3: Redacción resumen y conclusiones.**
        - **Descripción**: Se redacta el resumen y las conclusiones.
        - **Objetivos**: Redactar esta parte del documento.
        - **Duración**: 1 semana.
        - **Recursos**: Ingeniero –0.2 5 ingeniero/mes.
        - **Otros**: Posterior a E.2.

En la Tabla 7 se muestran estos datos.

Tarea	Duración (semanas)	Coste (Ing./mes)
Documentación y análisis del estado del arte.		
A.1: Estudio y análisis de redes inalámbricas	2	0,5
A.2: Estudio sobre monitorización y gestión de redes.	2	0,5
Subtotal		1
Despliegue red inalámbrica		
B.1: Estudio de los nodos inalámbricos, Fonera 2.0n	2	0,5
B.2: Actualización nodos inalámbricos	3	0,75
B.3: Configurar software en equipamiento	2	0,5
B.4 : Diseño de la red	4	1
B.5: Estudio herramientas visualización	4	1
B.6: Despliegue físico de los nodos	4	1
Subtotal		4,75
Obtención datos		
C.1: Configurar servidor	2	0,5
C.2: Configurar nodos	2	0,5
C.3: Puesta en funcionamiento del sistema y obtención de datos	4	1
Subtotal		2
Análisis de resultados		
D.1: Visualización de resultados en tiempo real	3	0,5
D.2: Mapas de gradiente	1	0,25
D.3: Graficas carga	1	0,25
Subtotal		1
Memoria		
E.1: Organización y estructura de la memoria.	1	0,25
E.2: Redacción de la memoria	4	1
E.3: Redacción resumen y conclusiones.	1	0,25
Subtotal		1,5
Total		10,25

Tabla 7 - Resumen descomposición de tareas

A.3 Planificación detallada

Una planificación más detallada de las fases de ejecución con su diagrama de Gantt se muestra en la Tabla 8 y en la Figura 21

Nombre de tarea	Duración	Conzo	Fin
Tarea A: Documentación y análisis del estado del arte.	**30 días**	**15/08/2012**	**25/09/2012**
A.1: Estudio y análisis de redes inalámbricas	11 días	15/08/2012	29/08/2012
A.2: Estudio sobre monitorización y gestión de redes.	10 días	30/08/2012	12/09/2012
Tarea B: Despliegue red inalámbrica	**96 días**	**26/09/2012**	**06/02/2013**
B.1: Estudio de los nodos inalámbricos, Fonera 2.0n	11 días	26/09/2012	10/10/2012
B.2: Actualización nodos inalámbricos	15 días	11/10/2012	31/10/2012
B.3: Configurar software en equipamiento	13 días	01/11/12	19/11/12
B.4 : Diseño de la red	23 días	20/11/12	20/12/12
B.5: Estudio herramientas visualización	24 días	21/12/12	23/01/13
B.6: Despliegue físico de los nodos	10 días	24/01/13	06/02/13
Tarea C :Obtención datos	**45 días**	**07/02/13**	**10/04/13**
C.1: Configurar servidor	15 días	07/02/13	27/02/13
C.2: Configurar nodos	15 días	07/02/13	27/02/13
C.3: Puesta en funcionamiento del sistema y obtención de datos	30 días	28/02/13	10/04/13
Tarea D: Análisis de resultados	**21 días**	**11/04/13**	**09/05/13**
D.1: Visualización de resultados en tiempo real	21 días	11/04/13	09/05/13
D.2: Mapas de gradiente	7 días	11/04/13	19/04/13
D.3: Graficas carga	7 días	11/04/13	19/04/13
Tarea E: Memoria	**31 días**	**10/05/13**	**21/06/13**
E.1: Organización y estructura de la memoria.	5 días	10/05/13	16/05/13
E.2: Redacción de la memoria	23 días	17/05/13	18/06/13
E.3: Redacción resumen y conclusiones.	3 días	19/06/13	21/06/13

Tabla 8 - Datos diagrama Gantt

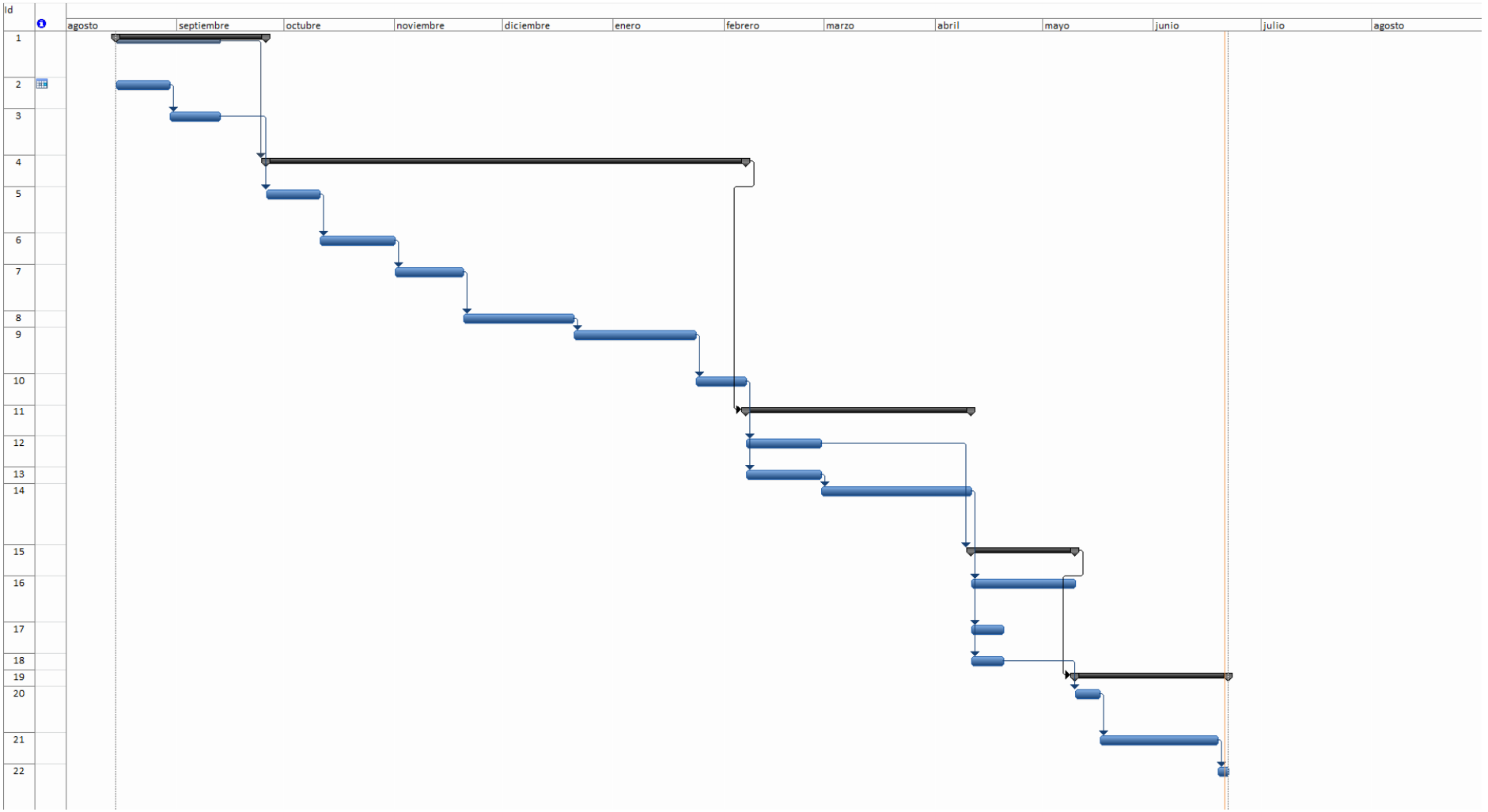


Figura 21 - Diagrama Gantt

A.3 Recursos

En este apartado se van a detallar los distintos recursos necesarios y usados para la realización de este Trabajo Fin de Grado.

- Recursos materiales:
  - Ordenador de sobremesa:
    - 1 PC Inter® Core® 2 Quad Processor Q940 @ 2.66GHz 4GB RAM. Sistema Operativo Debian 6 Squeeze.
  - Ordenador portátil:
    - 1 PC Intel® Core® i7 CPU Q720 € 160 GHz, 4GB de RAM. Sistema Operativo Windows 7 (64bits).
  - 14 nodos inalámbricos Fonera 2.0n (con cableado incluido).

- Recursos de trabajo:
  - 1 Graduado en Ingeniería Telemática: 6 ingenieros/mes.
  - 2 Ingenieros Senior: 0.5 ingenieros/mes.

- Otros costes:
  - Conexión a Internet durante 1 año.

A.1 Presupuesto del Proyecto

1. Autor: José María Montes Yuste
2. Departamento Ingeniería Telemática.
3. Descripción del Proyecto
   a. Título: Despliegue de una infraestructura para el análisis del tráfico 802.11.
   b. Duración: 1 año.
   c. Tasa de costes indirectos: 20%.
4. Presupuesto total del Proyecto: ver Tabla 9
5. Subcontratación de tareas: No se especifica.
6. Otros costes indirectos: No se especifica.

Concepto	Cantidad (€)	Coste (€)	% Proyecto	Dedicación (meses)	Depreciación (meses)	Total (€)
Recursos materiales						
Ordenadores sobremesa	1	550	100	12	60	330.00
Ordenadores portátiles	1	899	100	12	60	539.40
Nodos inalámbricos	14	1106	100	12	120	1.078,35
Subtotal						**1.947,75**
Recursos de trabajo						
Graduado Ing. Telemática	1(6 Ing./mes)	2694.39	-	-	-	16.166,34
Ingenieros Senior	2 (0.5 Ing./mes)	4289.54	-	-	-	2.144,77
Subtotal						**18.311,11**
Otros costes						
Conexión a Internet	1	30	-	12	-	360
Subtotal						**360**
Total						20.618,86€

Tabla 9 - Presupuesto

B. Instalación OpenWrt en los nodos

B.1 Firmware OpenWrt

OpenWrt define un firmware con distribución Linux para dispositivos integrados. El firmware es un bloque de instrucciones de programa para un fin concreto, almacenado en una memoria no volátil, que define a bajo nivel la lógica que controla los circuitos de un dispositivo electrónico. Esto es, que el firmware es el nexo – interfaz – entre las órdenes que se le dan a un dispositivo electrónico y la electrónica que las realiza. Como se ha mencionado anteriormente se puede encontrar en memorias no volátiles tipo ROM, flash, pero también incluso en los microprocesadores o chips. El firmware OpenWrt tiene la peculiaridad de ser libre, además está basado en GNU/Linux y optimizado para routers con reducida capacidades, como es el caso de nuestros nodos.

Figura 22 – Web OpenWrt

B.2 Routers Fonera

Los nodos elegidos pertenecen al proyecto FON, que conforma la mayor comunidad WiFi del mundo [11] , en particular las Fonera 2.0. Gracias a sus nodos o routers inalámbricos, comúnmente conocidos como Foneras, los usuarios pueden compartir parte de su ancho de banda de Internet con cualquier usuario de la comunidad FON. De este modo los miembros de esta comunidad pueden acceder de forma gratuita a los puntos de acceso FON de todo el mundo. Actualmente cuenta con más de 8 millones de puntos de acceso repartidos por todo el mundo.

Figura 23 - Fonera 2.0n

B.3 Proceso de cambio de firmware

A continuación se va a proceder a explicar el proceso de actualización para instalar el firmware de OpenWrt con su versión más actualizada, Attitude Adjustment r33265. Que es una de las líneas de desarrollo del firmware, en concreto la que soporta más arquitecturas.

El primer paso consiste instalar en la Fonera una versión base de OpenWrt, para ello:

- Conectamos la Fonera directamente al ordenador, mediante el uso del cable Ethernet, provisto por el fabricante, a una de la interfaces del routers – a excepción de la de Internet- como muestran las Figura 24 y Figura 25. Se asigna a la interfaz del ordenador donde ha sido conectada la Fonera una dirección IP de la subred 192.168.10.0/24, puesto que las interfaces del router tienen asignado por defecto la dirección 192.168.10.1/24 a modo de bridge.

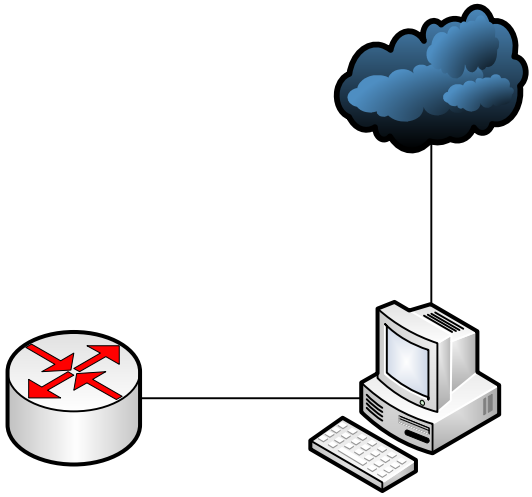


Figura 24 - Diagrama para actualizar Fonera

Figura 25 - Diagrama conexión cableado Fonera

- Nos descargamos la versión base de OpenWrt en el servidor, accesible desde http://download.fonosfera.org/Gari/20100408_FON2303_2.3.6.0_r1665_DEV.tgz.

- Accedemos a la Fonera, para ello es suficiente poner en el navegador http://192.168.10.1, para acceder a la interfaz web de la Fonera. La contraseña por defecto que traen los routers es *admin*, los pasos anteriores a la introducción de esta contraseña se deben omitir. Una vez dentro de la interfaz (Figura 26) vamos a Settings/System y en la parte de Actualización de firmware seleccionamos el archivo descargado en el punto anterior y le damos a upgrade. El proceso de actualización tarde cinco minutos.

sudo ip addr add 192.168.10.15/24 dev eth3

Figura 26 - Interfaz Fonera

Una vez llegados a este punto tenemos nuestra Fonera con firmware OpenWrt, en los siguientes puntos se procede a explicar el mecanismo para instalar el kernel más nuevo, 3.3.8.

- Debemos en primer lugar conectar la Fonera a Internet, mediante su Interfaz destinada a tal fin. Posteriormente debemos acceder a la Fonera mediante SSH.

ssh root@192.168.10.1

Una vez dentro debemos situarnos en el directorio temporal, descargar la nueva versión de kernel. Montar una imagen e instalarla, se detallan los pasos a seguir.

cd /tmp
wget http://erriko.it/download/fonera/openwrt/openwrt-fonera20n-r33265-240812.bin
mv openwrt-fonera20n-r33265-240812.bin fon20nopenwrt.bin
mtd -r write fon20nopenwrt.bin image

Figura 27 - Primera versión OpenWrt

- Esto cambia la dirección IP de las interfaces de la Fonera, por lo que es necesario reconfigurar en el PC una perteneciente a la nueva subred, que es la 192.168.1.1/24. Ahora se debe conectar por telnet la Fonera

sudo ip addr add 192.168.1.15/24 dev eth3
telnet 192.168.1.1

Se le pone una contraseña de administrador a la Fonera por seguridad y para poder acceder a ellas de modo más seguro por ssh, con el comando passwd.

- Una vez hecho esto se puede acceder por ssh a las Foneras ya con su versión de OpenWrt actualizada.

```
jmmontes@babosa:~$ ssh root@163.117.140.251


BusyBox v1.19.4 (2012-08-24 01:58:10 CEST) built-in shell (ash)
Enter 'help' for a list of built-in commands.

  _______                     ________        __
 |       |.-----.-----.-----.|  |  |  |.----.|  |_
 |   -   ||  _  |  -__|     ||  |  |  ||   _||   _|
 |_______||   __|_____|__|__||________||__|  |____|
          |__| W I R E L E S S   F R E E D O M
 -----------------------------------------------------
 ATTITUDE ADJUSTMENT (Bleeding Edge, r33265)
 -----------------------------------------------------
  * 1/4 oz Vodka      Pour all ingredients into mixing
  * 1/4 oz Gin        tin with ice, strain into glass.
  * 1/4 oz Amaretto
  * 1/4 oz Triple sec
  * 1/4 oz Peach schnapps
  * 1/4 oz Sour mix
  * 1 splash Cranberry juice
 -----------------------------------------------------
root@OpenWrt:~#
```

Figura 28- Versión final OpenWrt

B.4 Configuración interna básica

Para poder acceder de manera local a las Fonera una vez desplegadas se le han asignado a sus interfaces direcciones IP estáticas de una subred dedicada a tal fin, 10.7.23.0/24. Para ello se debe modificar el archivo */etc/config/network* así como separar las interfaces asociadas por un bridge.

```
config interface 'loopback'
        option ifname 'lo'
        option proto 'static'
        option ipaddr '127.0.0.1'
        option netmask '255.0.0.0'

config interface 'lan'
        option ifname 'eth0.1'
        #option type 'bridge'
        option proto 'static'
        option ipaddr '10.7.23.9'
        option netmask '255.255.255.0'
        option macaddr '00:18:84:89:3f:88'

config interface 'wan'
        option ifname 'eth0.2'
        option proto 'dhcp'
        option macaddr '00:18:84:89:3f:89'
```

Figura 29 - Archivo /etc/config/network

- Debemos habilitar la interfaz inalámbrica desde */etc/config/wirele* , comentando la línea que indica.

```
config wifi-device  radio0
        option type     mac80211
        option channel  11
        option macaddr  00:18:84:89:3f:8a
        option hwmode   11g
        #option htmode  HT20
        #list ht_capab  GF
        #list ht_capab  SHORT-GI-20
        #list ht_capab  SHORT-GI-40
        #list ht_capab  TX-STBC
        #list ht_capab  RX-STBC12
        # REMOVE THIS LINE TO ENABLE WIFI:
        #option disabled 1

config wifi-iface
        option device   radio0
        #option network  lan
        option mode     sta
        option ssid     Uni3
        option encryption none
```

Figura 30 - Archivo /etc/config/wireless

B.5 Instalación de paquetes y configuración complementaria

Para el correcto diseño del sistema se han necesitado una serie de paquetes auxiliares que no trae el firmware de serie. Los paquetes se obtienen gracias a la librería opkg. Los pasos que han sido necesarios seguir han sido:

- Actualizar la librería

opkg update

- Instalación de paquetes

opkg install ip
opkg instal kmod-fuse
opkg install fuse-utils
opkg install sshfs
opkg install ntfs-3g
opkg install tcpdump
opkg install bc

- Para la conexión de manera automática, sin necesidad de introducir claves manualmente, se han generado las parejas de clave publicas/privadas en ambos lados de la conexión (nodo y servidor) y se han intercambiado, para poder conectarse en remoto de manera bidireccional son introducir claves.

Para la conexión desde la Fonera hasta el PC: se generan las claves en el servidor y se guardan en los nodos.

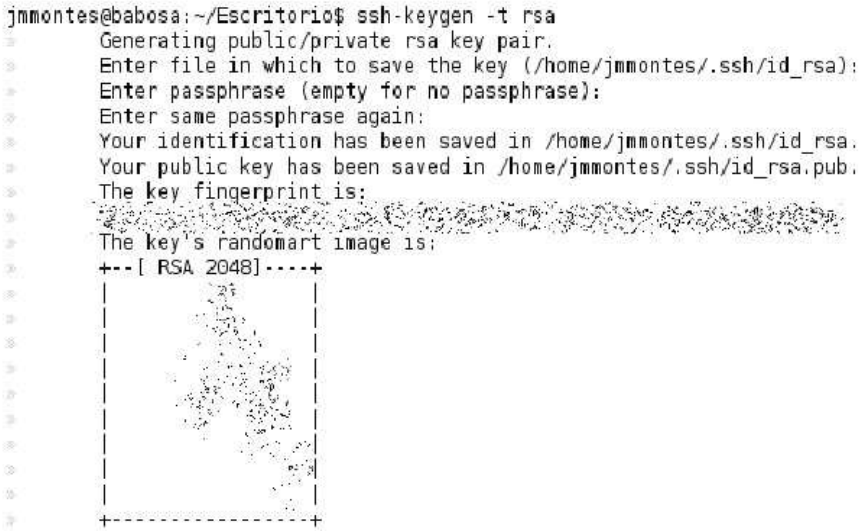


Figura 31 - Generación claves servidor

scp ~/.ssh/id_rsa.pub root@192.168.1.1:/tmp

Desde la Fonera:

Cd /etc/dropbear
Cat /tmp/id_*.pub >> authorized_keys
Chmod 0600 authorized_keys

Para la conexión el servidor hasta Fonera se generan las claves en la Fonera y se pasan al servidor guardándolo en el directorio *.ssh/authorized_keys*.

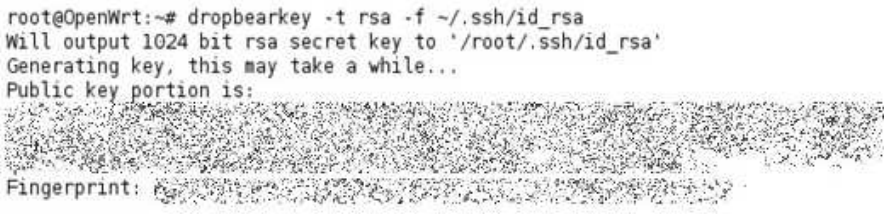


Figura 32 - Generación claves nodos

Glosario

La lista se acrónimos que ha sido utilizados en la memoria del Trabajo Fin de Grado han sido:

AP Access Point

API Application Programming Interface

DHCP Dynamic Host Configuration Protocol

FUSE Filesystem in USErspace

HTML HyperText Markup Lenguage

IEEE Institute of Electrical and Electronics Engineers

IP Internet Protocol

MAC Media Access Control

NIC Network Interface Card

NTP Network Time Protocol

OS Operative System

PC Personal Computer

PDA Personal Digital Assistant

SSH Secure SHell

SSHFS Secure SHell FileSystem

ST Station

USB Universal Serial Bus

UTC Universal Time Coordinated

VoIP Voice over IP

WiFi Wireless Fidelity

WLAN Wireless Local Area Network

Bibliografía

[1] I. C. Society, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 2012.

[2] M. S. Gast, Wireless Networks: The Definitive Guide, O'Reilly, 2002.

[3] CISCO, "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017," 2013.

[4] F. Halsall, Redes de Computadores e Internet, Pearson Education S.A, 2006.

[5] I. F. Akyildiz, "Wireless mesh networks: a survey," 2005.

[6] J. F. Kurose, Redes de computadoras. Un enfoque descendente, Pearson S.A, 2010.

[7] W. Stalling, Comunicaciones y Redes de Computadores, Pearson Sducación S.A, 2004.

[8] P. D. Denteneer, "The IEEE 802.11 Universe".

[9] Y.-C. Cheng, "Jigsaw: Solving the Puzzle of Enterprise 802.11 Analysis".

[10] E. Press, "El 40% de los ordenadores ha sufrido ataques de malware en el primer trimestre," *elEconomista,* 10 junio 2013.

[11] A. P. Jardosh, "Understanding Congestion in IEEE 802.11b Wireless Networks".

[12] U. Deshpande, "Refocusing in 802.11 Wireless Measurement".

[13] Fon, "Corporacion Fon," [Online]. Available: http://corp.fon.com/.

[14] "OpenWrt Wireless Freedom," [Online]. Available: https://openwrt.org/.

[15] M. Szeredi, "SSH Filesystem," [Online]. Available: http://fuse.sourceforge.net/sshfs.html.

[16] L. M. Garcia, "TCPDUMP & LIBCAP," [Online]. Available: http://www.tcpdump.org/.

[17] "Manual TShark," [Online]. Available: http://www.wireshark.org/docs/man-pages/tshark.html.

[18] "Network Time Protocol," [Online]. Available: http://datatracker.ietf.org/wg/ntp/charter/.

[19] "Highcharts," [Online]. Available: http://www.highcharts.com/.

[20] "OpenSSH," [Online]. Available: www.openssh.org.

[21] "Linux Wireless," [Online]. Available: http://wireless.kernel.org/en/users/Documentation.

[22] "Socket IO," [Online]. Available: http://socket.io/.

[23] A. Kvalbein, "The Nornet Edge platform for mobile broadband measurements".

[24] A. F. Molisch, Wireless communications, John Wiley & Sons, 2011.

[25] W. Webb, Wireless communications : the future, John Wiley & Sons, 2007.

[26] T. Bradley, Wireless Security: Know It All.

[27] R. Temple, Internet and wireless security, The Institution of Electrical Engineers, 2002.

[28] B. GILMER, Network monitoring, 2009.

[29] A. Ben Hamou, Practical Ruby for system administration.